Guida utente di HP Integrated Lights-Out 2

per firmware versione 1.75 e 1.77

Numero di parte 394326-069

Nona edizione (aprile 2009)

Destinatari

Questa guida è destinata a tutti coloro a cui è affidato il compito di installare, amministrare e curare la manutenzione dei server e dei sistemi di memorizzazione. L'installazione deve essere eseguita da personale qualificato in servizi di supporto ad apparecchiature informatiche e in grado di riconoscere i pericoli connessi all'utilizzo di prodotti che possono generare potenziali elettrici pericolosi.

Sommario

4 Utilizzo di iLO 2

1 Panoramica sul funzionamento

In questa sezione

Panoramica sulla guida

Il processore di gestione iLO 2 offre diversi metodi per configurare, aggiornare e utilizzare i server in remoto. Nella *Guida utente di HP Integrated Lights-Out 2* sono illustrate queste funzionalità e vengono descritte le procedure correlate da eseguire tramite l'interfaccia basata su browser e l'utility RBSU (ROM-Based Setup Utility). Alcune funzionalità richiedono una licenza e sono quindi accessibili solo dopo l'acquisto di una licenza opzionale. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20).

Nella *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out* vengono fornite informazioni sulla sintassi e sugli strumenti disponibili per utilizzare iLO 2 mediante una riga di comando o un'interfaccia di scripting.

Nella presente documentazione viene illustrato HP Integrated Lights-Out per server ProLiant ML/DL e server blade ProLiant BladeSystem. Per informazioni su iLO per server Integrity e server blade, visitare il sito Web HP all'indirizzo (http://www.hp.com/go/integrityiLO).

In questa guida sono incluse informazioni sul firmware di iLO 2 versione 1.11, 1.2x, 1.3x, 1.70, 1.75 e 1.77.

Nuove funzionalità disponibili in iLO 2

Nella versione 1.77 di iLO 2 è stato aggiunto il supporto avanzato per una modalità di alimentazione ad alta efficienza (HEM, High Efficiency Mode). Per ulteriori informazioni, vedere "Efficienza di alimentazione (Efficienza di alimentazione a pagina 130)".

Nella versione 1.75 di iLO 2 sono state aggiunte le seguenti funzionalità:

- Supporto per modello di licenza - iLO2 offre licenze iLO Advanced e iLO Advanced for BladeSystem come aggiornamenti acquistabili per le funzionalità standard di gestione remota disponibili su HP ProLiant e BladeSystem. Per ulteriori informazioni, visitare il sito Web HP (http://www.hp.com/go/ilo).
- Supporto migliorato per gli account di directory fino a 15 contesti di ricerca.
- Supporto dei servizi di directory per Active Directory di Windows 2008.

- Creazione di rapporti sullo stato della temperatura delle unità, quando supportato dalla piattaforma.
- Server aggiuntivi:
  - ProLiant BL260c G6
  - ProLiant BL460c G6
  - ProLiant BL490c G6
  - ProLiant DL320 G6
  - ProLiant DL360 G6
  - ProLiant DL380 G6
  - ProLiant ML310 G5p
  - ProLiant ML330 G6
  - ProLiant ML350 G6
  - ProLiant ML370 G6

Panoramica su iLO 2

iLO 2 consente di eseguire in remoto molte delle funzioni che generalmente richiedono un intervento manuale su server collocati all'interno di datacenter, sale macchine o sedi remote. Di seguito sono riportati alcuni esempi di utilizzo di iLO 2.

- Mediante l'opzione di accensione virtuale e la console remota di iLO 2, è possibile esaminare i server remoti nei quali è stato generato un evento di blocco con schermata blu e riavviare il server senza dover prestare assistenza onsite.
- La console remota di iLO 2 consente di modificare, se necessario, le impostazioni del BIOS.
- La console remota ad alte prestazioni basata sulla tecnologia iLO 2 Virtual KVM consente di eseguire in remoto le normali attività di gestione di sistemi operativi e applicazioni.
- La funzione di unità dischetto o CD/DVD-ROM virtuale offerta da iLO 2 consente di eseguire in rete l'installazione di un sistema operativo o la programmazione del firmware di un sistema utilizzando immagini software disponibili nella propria workstation o in un server Web centralizzato.
- La cartella virtuale di iLO 2 consente di aggiornare i driver del sistema operativo o di copiare i file di sistema senza disporre di supporti fisici né creare un'immagine del disco.
- Lo scripting di iLO 2 consente di utilizzare la funzione di accensione virtuale e i supporti virtuali in altri strumenti di scripting per la distribuzione e il provisioning automatici.
- iLO 2 partecipa attivamente alle fasi di monitoraggio e controllo dello stato del server, indicato con il termine stato integrato. iLO 2 controlla le temperature nel server e invia segnali correttivi alle ventole in modo da garantire il raffreddamento corretto del server. Oltre al controllo della temperature, iLO 2 consente il monitoraggio dello stato delle ventole, degli alimentatori, dei moduli di regolazione della tensione e delle unità disco rigido interne.

Gli esempi descritti illustrano solo alcuni casi di utilizzo di iLO 2 per gestire i server HP ProLiant in ufficio, a casa o in viaggio. Per gli utenti che iniziano a utilizzare iLO 2 e a definire i requisiti dell'infrastruttura, consultare la presente guida per informazioni su procedure aggiuntive utili per semplificare le attività di gestione remota dei server.

Per informazioni sulle funzionalità disponibili in ciascuna versione di iLO 2, vedere la sezione "Licenze" (Licenze a pagina 20).

Principali differenze tra iLO e iLO 2

iLO 2 è basato su iLO, con il quale condivide molte funzionalità. Tuttavia, per utilizzare iLO 2 per l'accesso a una console remota basata su testo prima dell'avvio del sistema operativo, è necessario utilizzare la console seriale remota. Per ulteriori informazioni, vedere la sezione "Panoramica sulla console remota basata su testo" (Panoramica sulla console remota basata su testo a pagina 104).

Di seguito sono messe in evidenza le differenze tra iLO 2 e iLO:

Funzione	iLO 2	iLO (Porta: iLO)
Funzionalità standard		
Console di testo	Pre-SO	Pre-SO e SO
Console seriale remota (porta seriale virtuale)	Pre-SO e SO	Pre-SO e SO
Monitoraggio e controllo dello stato del server	Sì	No
Funzionalità avanzate		
Console di testo	Pre-SO e SO	Pre-SO e SO
Console remota	Sì (Virtual KVM)	Sì
Console remota integrata	Sì	No
Supporto per Microsoft® JVM	Sì	No
Pulsante Remote Console Acquire (Acquisizione console remota)	Sì	Sì
Integrazione di Servizi terminal	Sì	Sì
Integrazione delle directory tramite schema HP	Sì	Sì
Integrazione delle directory senza schema	Sì	Sì
Autenticazione basata su due fattori	Sì	Sì
Report del regolatore di alimentazione	Sì	Sì
CD/DVD-ROM e dischetto virtuali	Sì	Sì
Supporti virtuali chiave USB	Sì	Sì
Cartella virtuale	Sì	No

Integrazione di HP Insight Essentials Rapid Deployment Pack

HP Insight Essentials Rapid Deployment Pack è integrato con iLO 2 e consente la gestione dei server remoti e l'esecuzione delle operazioni della console remota indipendentemente dallo stato del sistema operativo o dell'hardware.

Il Deployment Server (Server di distribuzione) consente di utilizzare le funzioni di gestione dell'alimentazione di iLO 2 per accendere, spegnere oppure spegnere e riaccendere il server di destinazione. Quando un server si collega al Deployment Server, questo esegue il polling del server di destinazione per individuare la presenza di un dispositivo di gestione LOM. Se il dispositivo è installato, il server raccoglie le informazioni, quali il nome DNS, l'indirizzo IP e il primo nome utente. La funzione

di protezione richiede all'utente l'immissione della password corretta corrispondente al nome utente rilevato.

Per ulteriori informazioni su Insight Essentials Rapid Deployment Pack, consultare la documentazione fornita con il CD di Insight Essentials Rapid Deployment Pack oppure visitare il sito Web HP all'indirizzo http://www.hp.com/servers/rdp.

Gestione del server mediante applicazioni compatibili con IPMI versione 2.0

La gestione del server mediante l'interfaccia IPMI è un metodo standard per il controllo e il monitoraggio del server. iLO 2 fornisce funzionalità di gestione del server basate sulle specifiche dell'interfaccia IPMI versione 2.0.

Le specifiche IPMI definiscono un'interfaccia standardizzata per la gestione delle piattaforme, in particolare:

- Monitoraggio delle informazioni di sistema, quali dati relativi a ventole, temperature e alimentatori.
- Funzionalità di ripristino, ad esempio reimpostazione del sistema e operazioni di accensione/ spegnimento.
- Funzionalità di registrazione, per eventi eccezionali quali temperature eccessive o guasti delle ventole.
- Funzionalità di inventario, ad esempio identificazione di componenti hardware guasti.

Le comunicazioni IPMI dipendono dal controller BMC e dal server SMS. Il controller BMC gestisce l'interfaccia tra il server SMS e l'hardware di gestione della piattaforma. iLO 2 emula le funzionalità del controller BMC, mentre le funzionalità del server SMS possono essere fornite mediante vari strumenti standard del settore. Per ulteriori informazioni, fare riferimento alle specifiche dell'interfaccia IPMI sul sito Web Intel® all'indirizzo http://www.intel.com/design/servers/ipmi/tools.htm.

iLO 2 fornisce l'interfaccia KCS, o interfaccia aperta, per le comunicazioni del server SMS, che include un insieme di registri di comunicazione associati agli I/O. L'indirizzo di base di sistema predefinito per l'interfaccia SMS associata agli I/O è 0xCA2 e l'interfaccia è allineata a livello di byte con questo indirizzo di sistema.

L'interfaccia KCS è accessibile al software SMS in esecuzione sul sistema locale. Di seguito sono elencate alcune applicazioni software compatibili con SMS:

- Command Test Tool dell'interfaccia IPMI versione 2.0 è uno strumento a basso livello da riga di comando MS-DOS che consente di inviare comandi IPMI in formato esadecimale a un controller BMC IPMI che implementa l'interfaccia KCS. Questo strumento è disponibile sul sito Web Intel® all'indirizzo http://www.intel.com/design/servers/ipmi/tools.htm.
- IPMItool è un'utility per la gestione e la configurazione di dispositivi che supportano le specifiche IPMI versione 1.5 e 2.0 e può essere utilizzato in un ambiente Linux. Questo strumento è disponibile sul sito Web IPMItool all'indirizzo http://ipmitool.sourceforge.net/index.html.

Funzionalità IPMI fornite da iLO 2

Quando emula un controller BMC per l'interfaccia IPMI, iLO 2 supporta tutti i comandi richiesti elencati nelle specifiche IPMI versione 2.0. Fare riferimento alle specifiche dell'interfaccia IPMI versione 2.0 per un elenco di questi comandi. Il server SMS deve inoltre utilizzare i metodi descritti nelle specifiche per determinare quali funzionalità IPMI sono abilitate e quali sono disabilitate nel controller BMC, ad esempio utilizzando il comando Get Device ID.

Se il sistema operativo del server è in esecuzione e il driver di sicurezza è abilitato, il traffico IPMI che passa tramite l'interfaccia KCS può influenzare le prestazioni del driver di sicurezza e quelle globali del sistema. Non utilizzare l'interfaccia KCS per inviare comandi IPMI che potrebbero avere un effetto

negativo sul monitoraggio effettuato dal driver di sicurezza. Tra questi comandi sono inclusi quelli che impostano o modificano i parametri IPMI, quali `Set Watchdog Timer` e `Set BMC Global Enabled`. Non creano invece problemi i comandi IPMI che restituiscono dati, ad esempio `Get Device ID` e `Get Sensor Reading`.

Panoramica sulla compatibilità di WS-Management

L'implementazione del firmware di iLO 2 di WS-Management è conforme alle specifiche DTMF *Web Services for Management* 1.0.0a.

Autenticazione

- iLO 2 utilizza l'autenticazione di base su SSL, in conformità al seguente profilo: `wsman:secprofile/https/basic`
- Gli utenti autenticati sono autorizzati a eseguire i comandi di WS-Management in conformità ai privilegi designati nei rispettivi account locali o di directory.
- Per abilitare l'autenticazione di base in Microsoft® Windows Vista™, al prompt dei comandi immettere `gpedit.msc` per avviare Editor oggetti Criteri di gruppo. Selezionare **Configurazione computer>Modelli amministrativi>Componenti di Windows>Gestione remota Windows>Client Gestione remota Windows**. Impostare Consenti autenticazione di base su **Abilitata**.

Compatibilità

- L'implementazione di WS-Management in iLO 2 è compatibile con l'utility WinRM di Windows Vista™, Microsoft® Operations Manager 3 e il Management Pack fornito da HP.
- L'insieme completo dei comandi di WS-Management è disponibile sui server iLO 2 con supporto incorporato per la sicurezza del sistema. Un insieme notevolmente ridotto dei comandi è disponibile sui server che sono privi di tale supporto.

Sono disponibili comandi per richiamare in remoto i seguenti dispositivi:

- Alimentatore del server
- UID

Stato

L'implementazione di WS-Management in iLO 2 restituisce le informazioni sullo stato per ventole, temperature, alimentatori e VRM.

Panoramica sull'interfaccia del browser Web di iLO 2

Per semplificare la navigazione e la gestione del flusso di lavoro, nell'interfaccia del browser di iLO 2 le attività simili sono raggruppate all'interno di schede generali visualizzate nella parte superiore dell'interfaccia. Visibili sempre in primo piano, queste schede comprendono System Status (Stato sistema), Remote Console (Console remota), Virtual Media (Supporti virtuali), Power Management (Gestione alimentazione) e Administration (Amministrazione).

A ogni scheda di iLO 2 è associato un menu specifico contenente varie opzioni, visualizzato nella parte sinistra dell'interfaccia. Il menu cambia a seconda della scheda selezionata e riflette le opzioni disponibili all'interno della scheda. Se si seleziona un'opzione, viene visualizzato un titolo di pagina, ovvero una descrizione delle informazioni o delle impostazioni disponibili all'interno della pagina. Il titolo potrebbe non corrispondere esattamente al nome dell'opzione di menu.

Ulteriori informazioni su tutte le opzioni di iLO 2 sono disponibili tramite la relativa Guida in linea. I collegamenti presenti nelle pagine di iLO 2 consentono di accedere a informazioni di riepilogo sulle

funzionalità di iLO 2 e a dati utili per l'ottimizzazione delle operazioni. Per accedere a una pagina specifica della guida, fare clic sul **punto interrogativo (?)** sul lato destro della finestra del browser.

Le attività normalmente svolte dagli utenti prevedono l'utilizzo delle schede System Status (Stato sistema), Remote Console (Console remota), Virtual Media (Supporti virtuali) e Power Management (Gestione alimentazione) dell'interfaccia di iLO 2. Queste attività sono illustrate nella sezione "Utilizzo di iLO 2" (Utilizzo di iLO 2 a pagina 78).

La scheda Administration (Amministrazione) è in genere utilizzata da utenti di livello avanzato o dotati di privilegi amministrativi, che hanno il compito di gestire gli utenti, configurare le impostazioni globali e di rete, nonché configurare o abilitare le funzioni più avanzate di iLO 2. Queste attività sono illustrate nelle sezioni "Impostazione di iLO 2" (Impostazione di iLO 2 a pagina 8) e "Configurazione di iLO 2" (Configurazione di iLO 2 a pagina 17).

Argomenti specifici relativi alle funzionalità e all'integrazione di iLO 2 sono illustrati nelle seguenti sezioni:

- Servizi di directory (Servizi di directory a pagina 145)
- Gestione remota abilitata alla directory (Gestione remota abilitata alla directory a pagina 179)
- Utility di migrazione delle directory HPQLOMIG (Utility di migrazione delle directory HPQLOMIG a pagina 187)
- Integrazione di HP Systems Insight Manager (Integrazione di HP Systems Insight Manager a pagina 199)
- Risoluzione dei problemi relativi a iLO 2 (Risoluzione dei problemi relativi a iLO 2 a pagina 205)
- Schema dei servizi di directory (Schema dei servizi di directory a pagina 233)

Browser e sistemi operativi client supportati

- Microsoft® Internet Explorer 7
  - Questo browser è supportato solo su prodotti con Microsoft® Windows®.
  - Sono supportati Microsoft® JVM e SUN Java™ 1.4.2_13. Dal sito Web HP è possibile scaricare l'applicazione JVM più adatta alla propria configurazione di sistema (http://www.hp.com/servers/manage/jvm).
- Microsoft® Internet Explorer 6 con Service Pack 1 o successivo
  - Questo browser è supportato solo su prodotti con Microsoft® Windows®.
  - Sono supportati Microsoft® JVM e SUN Java™ 1.4.2_13. Dal sito Web HP è possibile scaricare l'applicazione JVM più adatta alla propria configurazione di sistema (http://www.hp.com/servers/manage/jvm).
- Firefox 2.0
  - Questo browser è supportato su Red Hat Enterprise Linux Desktop 4 e Novell Linux Desktop 9.
  - Sono supportati Microsoft® JVM e SUN Java™ 1.4.2_13. Dal sito Web HP è possibile scaricare l'applicazione JVM più adatta alla propria configurazione di sistema (http://www.hp.com/servers/manage/jvm).

Alcune combinazioni di browser e sistemi operativi potrebbero non funzionare correttamente a seconda dell'implementazione delle tecnologie di browser richieste.

Software del sistema operativo del server supportato

iLO 2 è un microprocessore indipendente con sistema operativo incorporato. Questa architettura garantisce la disponibilità della maggior parte delle funzionalità di iLO 2, indipendentemente dal sistema operativo dell'host utilizzato.

Per consentire il normale arresto del sistema operativo del server host, l'integrazione di HP SIM richiede driver di sicurezza e Management Agents oppure l'accesso alla console remota.

iLO 2 comprende due driver di interfaccia:

- iLO 2 Advanced Server Management Controller Driver (driver di sicurezza) – Fornisce il supporto per la gestione del sistema, incluso il monitoraggio dei componenti del server, la registrazione degli eventi e il supporto di Management Agents.
- iLO 2 Management Interface Driver – Consente al software del sistema e SNMP Insight Agents di comunicare con iLO 2.

Questi driver e agenti sono disponibili per i seguenti sistemi operativi di rete:

- Microsoft®
  - Windows® 2008 Server
  - Windows® 2008 Advanced Server
  - Windows Server® 2003
  - Windows Server® 2003, Web Edition
  - Windows® Small Business Server 2003 (serie ML300)
  - Windows Vista®
- Red Hat
  - RedHat Enterprise Linux 3 (x86)
  - Red Hat Enterprise Linux 3 (AMD64/EM64T)
  - RedHat Enterprise Linux 4 (x86)
  - Red Hat Enterprise Linux 4 (AMD64/EM64T)
  - RedHat Enterprise Linux 5 (x86)
  - Red Hat Enterprise Linux 5 (AMD64/EM64T)
- SUSE
  - SUSE LINUX Enterprise Server 9 (x86)
  - SUSE LINUX Enterprise Server (AMD64/EM64T)
  - SUSE LINUX Enterprise Server 10

2 Impostazione di iLO 2

In questa sezione

Impostazione rapida

Per configurare rapidamente iLO 2 utilizzando le impostazioni predefinite per le funzionalità di iLO 2 Standard e iLO Advanced, effettuare le operazioni descritte nei passaggi riportati di seguito:

1. Preparazione: stabilire la modalità di gestione della rete e della protezione (vedere la sezione Preparazione per l'impostazione di iLO 2 a pagina 9).
2. Connettere iLO 2 alla rete (vedere la sezione Connessione alla rete a pagina 11).
3. Se non si dispone di un indirizzo IP dinamico, utilizzare l'utility RBSU di iLO 2 per configurare un indirizzo IP statico (vedere la sezione Configurazione dell'indirizzo IP a pagina 11).
4. Accedere a iLO 2 tramite un browser supportato o una riga di comando utilizzando le informazioni predefinite di nome utente, password e nome DNS riportate sull'etichetta delle impostazioni di rete di iLO 2 presente sul server (vedere la sezione Primo accesso a iLO 2 a pagina 12).
5. Modificare il nome utente e la password predefiniti per l'account amministratore specificando le selezioni desiderate.
6. Se si utilizza la funzionalità degli account locali, impostare gli account utente (vedere la sezione Impostazione degli account utente a pagina 12).
7. Attivare le funzionalità avanzate di iLO 2 (vedere la sezione Attivazione mediante browser delle funzionalità di iLO 2 per cui è necessaria la licenza a pagina 13).
8. Installare i driver di iLO 2 (vedere la sezione Installazione dei driver di iLO 2 a pagina 14).

Preparazione per l'impostazione di iLO 2

Prima di impostare il processore di gestione iLO 2, è necessario scegliere il tipo di configurazione che si desidera utilizzare per la connessione di rete e le impostazioni di protezione. Di seguito sono riportate alcune domande che possono essere utili per configurare iLO 2 in base alle proprie esigenze:

1. In che modo è possibile connettere iLO 2 in rete? Per una rappresentazione grafica e una descrizione delle modalità di connessione disponibili, vedere la sezione "Connessione in rete" (Connessione alla rete a pagina 11).

   In genere sono disponibili due metodi per la connessione di iLO 2 in rete:

   - Tramite una rete aziendale, a cui sono connessi sia il controller di rete che la porta iLO 2. Questa connessione consente di accedere a iLO 2 da qualsiasi punto della rete e di ridurre l'hardware e l'infrastruttura necessari per il supporto di iLO 2. Tuttavia, il traffico di una rete aziendale può determinare una riduzione delle prestazioni di iLO 2.

   - Tramite una rete di gestione dedicata, con la porta iLO 2 su una rete separata. Quest'ultima consente di migliorare le prestazioni e la sicurezza poiché è possibile controllare fisicamente le workstation connesse alla rete. Una rete separata garantisce inoltre l'accesso ridondante al server quando si verifica un guasto hardware sulla rete aziendale. In questa configurazione non è possibile accedere a iLO 2 direttamente dalla rete aziendale.

2. In che modo iLO 2 acquisisce un indirizzo IP?

   Per accedere a iLO 2 dopo la connessione alla rete, il processore di gestione deve acquisire un indirizzo IP e una maschera di sottorete tramite un processo dinamico o statico:

   - L'opzione Dynamic IP address (Indirizzo IP dinamico) è attivata per impostazione predefinita. iLO 2 ottiene l'indirizzo IP e la maschera di sottorete dai server DNS/DHCP. Questo è il metodo più semplice.

   - L'opzione Static IP address (Indirizzo IP statico) viene utilizzata per configurare un indirizzo IP statico se sulla rete non sono disponibili server DNS/DHCP. È possibile configurare un indirizzo statico in iLO 2 tramite l'utility RBSU.

     Se si utilizza un indirizzo IP statico, è necessario disporre di un indirizzo IP prima di iniziare l'impostazione di iLO 2.

3. Che tipo di protezione di accesso, privilegi e account utente sono richiesti?

   iLO 2 offre diverse opzioni per controllare l'accesso degli utenti. Per impedire l'accesso non autorizzato alle risorse IT dell'azienda è necessario selezionare uno dei seguenti metodi:

   - Memorizzare in iLO 2 account locali fino a un massimo di 12 password e nomi utente. Questo metodo rappresenta la soluzione ideale per gli ambienti di dimensioni ridotte, ad esempio i laboratori e le piccole e medie imprese.

   - Utilizzare la directory aziendale tramite servizi di directory (Microsoft® Active Directory o Novell eDirectory) per gestire l'accesso degli utenti a iLO 2. Questo metodo rappresenta la soluzione ideale per gli ambienti caratterizzati da un numero elevato di utenti che cambiano spesso. Si consiglia tuttavia di mantenere attivo almeno un account locale da utilizzare come accesso alternativo anche quando si decide di utilizzare i servizi di directory.

     Per ulteriori informazioni sulla protezione dell'accesso a iLO 2, vedere la sezione "Protezione" Protezione a pagina 38).

4. Come si desidera configurare iLO 2?

iLO 2 supporta varie interfacce per la configurazione e il funzionamento. In questa guida sono descritte in dettaglio le seguenti interfacce:

- RBSU di iLO 2 (vedere la sezione Impostazione di iLO 2 mediante l'utility RBSU a pagina 13). Questa utility può essere utilizzata quando l'ambiente di sistema non è basato su DHCP e DNS o WINS.
- Configurazione basata su browser (vedere la sezione Impostazione di iLO 2 mediante l'opzione basata su browser a pagina 13). Questo metodo può essere usato quando è possibile collegarsi a iLO 2 in rete mediante un browser e quando si desidera riconfigurare un processore iLO 2 già configurato.
- CLP SMASH. Questa interfaccia può essere utilizzata quando è possibile accedere a una riga di comando tramite Telnet, SSH o mediante una porta seriale fisica. Per informazioni, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

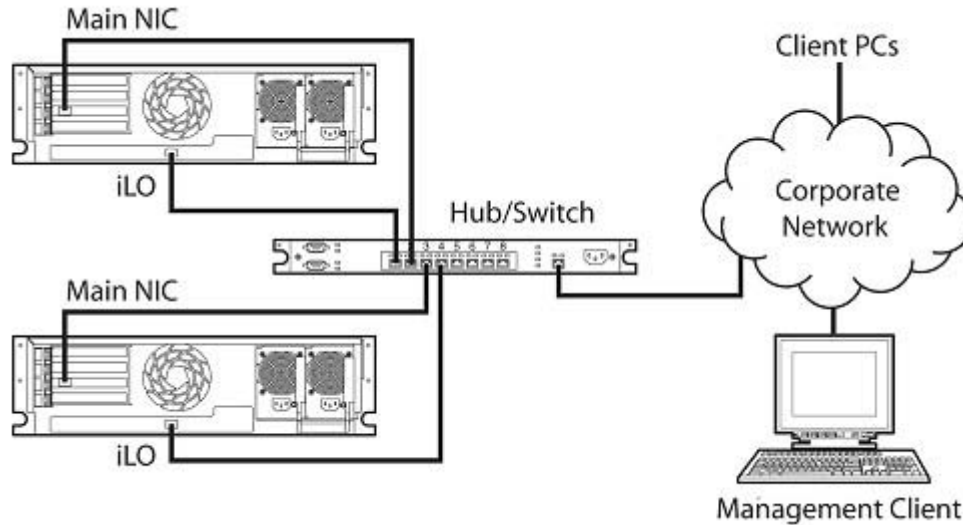
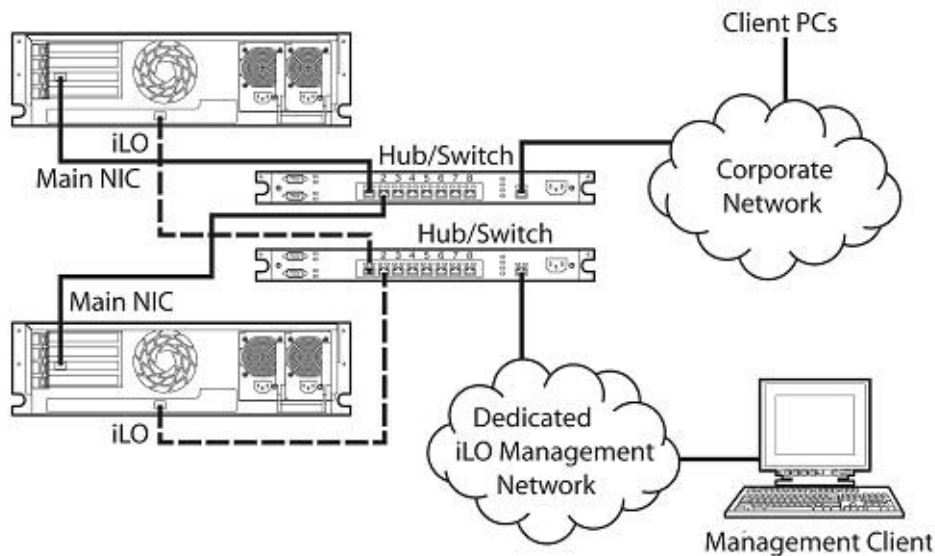
Le impostazioni predefinite di iLO 2 consentono di utilizzare la maggior parte delle funzionalità senza richiedere ulteriori operazioni di configurazione. Tuttavia, l'elevata flessibilità di configurazione che caratterizza iLO 2 permette di eseguire personalizzazioni specifiche per diversi ambienti aziendali. Per tutte le opzioni disponibili, vedere la sezione "Configurazione di iLO 2" (Configurazione di iLO 2 a pagina 17).

Di seguito sono riportati i metodi disponibili per l'impostazione avanzata di più processori di gestione iLO 2 mediante comandi di scripting. Gli script sono file di testo scritti in un linguaggio per script basato su XML chiamato RIBCL. È possibile utilizzare script RIBCL per configurare iLO 2 sulla rete, durante un'installazione iniziale o da un host già installato. Una descrizione dettagliata di ciascun metodo è disponibile nella *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

- CPQLOCFG è un'utility di Microsoft® Windows® che invia a iLO 2 gli script RIBCL tramite la rete.
- HPONCFG è un'utility in linea basata su scripting per la configurazione in locale che viene eseguita sul sistema host e trasferisce gli script RIBCL al processore iLO 2 locale. Questa utility è disponibile in versione per Windows® e per Linux e richiede l'installazione di HP iLO 2 Management Interface Driver.
- Perl è un linguaggio per script che può essere utilizzato dai client Linux per inviare a iLO 2 gli script RIBCL attraverso la rete.

Connessione alla rete

In genere sono disponibili due metodi per la connessione di iLO 2 in rete, ovvero tramite:

- **Rete aziendale** in cui entrambe le porte sono connesse alla rete aziendale. In questa configurazione, il server dispone di due porte di rete (un controller di rete del server e un controller di rete iLO 2) collegati a una rete aziendale.

- **Rete di gestione dedicata** in cui la porta di iLO 2 viene connessa a una rete separata.

Configurazione dell'indirizzo IP

È necessario eseguire questa operazione solo se si utilizza un indirizzo IP statico. Quando si utilizza un indirizzo IP dinamico, il server DHCP assegna automaticamente un indirizzo IP per iLO 2. Per semplificare l'installazione si consiglia di usare DNS o DHCP con iLO 2.

Per configurare un indirizzo IP statico, effettuare la seguente procedura con l'utility RBSU di iLO 2 per disabilitare DNS e DHCP e configurare l'indirizzo IP e la maschera di sottorete:

1. Riavviare o accendere il server.
2. Quando richiesto durante il POST, premere il tasto **F8**. L'utility RBSU di iLO 2 viene avviata.
3. Selezionare **Network**>**DNS/DHCP** (Rete>DNS/DHCP), quindi premere **Invio** e selezionare **DHCP Enable** (Abilitazione DHCP). Per disabilitare DHCP, premere la barra spaziatrice. Accertarsi che l'opzione DHCP Enable (Abilitazione DHCP) sia impostata su Off (Disattivata) e salvare le modifiche.
4. Selezionare **Network**>**NIC**>**TCP/IP** (Rete>NIC>TCP/IP), quindi premere **Invio** e immettere le informazioni appropriate nei campi IP Address (Indirizzo IP), Subnet Mask (Maschera di sottorete) e Gateway IP Address (Indirizzo IP del gateway).
5. Salvare le modifiche.
6. Chiudere l'utility RBSU di iLO 2. Le modifiche avranno effetto dopo la chiusura dell'utility.

Primo accesso a iLO 2

iLO 2 è configurato con un nome utente, una password e un nome DNS predefiniti. Le informazioni sull'utente predefinito si trovano sull'etichetta delle impostazioni di rete fissata al server che contiene il processore di gestione iLO 2. Utilizzare questi valori per accedere a iLO 2 in remoto da un client di rete mediante un browser Web standard.

Per motivi di sicurezza, HP consiglia di modificare le impostazioni predefinite dopo il primo accesso a iLO 2.

I valori predefiniti sono:

- User name (Nome utente) - Administrator
- Password - Una stringa alfanumerica di otto caratteri definita in modo casuale.
- DNS Name (Nome DNS) - *iLOXXXXXXXXXXXX*, dove le *X* rappresentano il numero di serie del server.

NOTA: Per i nomi utente e le password viene fatta distinzione tra maiuscole e minuscole.

Se si immette un nome utente e una password errati o in caso di tentativo di accesso non riuscito, iLO 2 impone un ritardo di protezione. Per ulteriori informazioni sulla protezione dell'accesso, vedere la sezione "Protezione dell'accesso" (Protezione dell'accesso a pagina 42).

Impostazione degli account utente

iLO 2 è preconfigurato con le impostazioni predefinite, comprendenti un account utente e una password predefiniti. Per motivi di sicurezza, HP consiglia di modificare le impostazioni predefinite dopo il primo accesso a iLO 2. Queste modifiche possono essere eseguite tramite una delle interfacce utente di iLO 2. Una descrizione dettagliata delle procedure tramite l'utility RBSU o basata su browser è disponibile nella presenta guida. Una descrizione delle altre opzioni, tra cui CLP SMASH, e dei metodi di scripting è disponibile nella *"Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out"*.

Se iLO 2 è collegato a una rete su cui è in esecuzione DNS o DHCP, può essere utilizzato immediatamente senza modificare le impostazioni.

Impostazione di iLO 2 mediante l'utility RBSU

HP raccomanda di ricorrere all'utility RBSU di iLO 2 per l'installazione e la configurazione iniziale di iLO 2 e dei relativi parametri di rete in ambienti che non utilizzano i protocolli DHCP e DNS o WINS. RBSU fornisce gli strumenti di base per configurare le impostazioni di rete iLO 2 e gli account utente per collegare iLO 2 in rete.

È possibile utilizzare RBSU per configurare parametri di rete, impostazioni di directory, impostazioni globali e account utente. L'utility RBSU di iLO 2 non è progettata per le attività di amministrazione continue. L'utility RBSU è disponibile a ogni avvio del server e può essere eseguita a distanza dalla console remota di iLO 2.

È possibile disabilitare l'RBSU di iLO 2 nelle preferenze relative alle impostazioni globali. In tal caso sarà possibile riconfigurare l'host solo se è azionato l'interruttore di annullamento della protezione di iLO 2.

Per eseguire l'utility RBSU di iLO 2 per configurare gli account locali:

1. Riavviare o accendere il server.
2. Quando richiesto durante il POST, premere il tasto **F8**. L'utility RBSU di iLO 2 viene avviata.
3. Se richiesto, immettere un ID utente iLO 2, provvisto dei privilegi iLO 2 appropriati, e una password validi in **Administer User Accounts>Configure iLO 2 Settings** (Amministra account utente>Configura impostazioni di iLO 2). Le informazioni sull'account predefinito si trovano sull'etichetta delle impostazioni di rete predefinite fissata al server che contiene il processore di gestione iLO 2. Se iLO 2 non è stato configurato in modo da richiedere l'identificativo di accesso all'utility RBSU, non verrà visualizzato alcun prompt.
4. Apportare le modifiche necessarie alla configurazione di iLO 2, quindi salvarle.
5. Chiudere l'utility RBSU di iLO 2.

Impostazione di iLO 2 mediante l'opzione basata su browser

Se è possibile collegarsi a iLO 2 in rete mediante un browser, usare il metodo di configurazione basato su browser, anche per riconfigurare un iLO 2 già configurato.

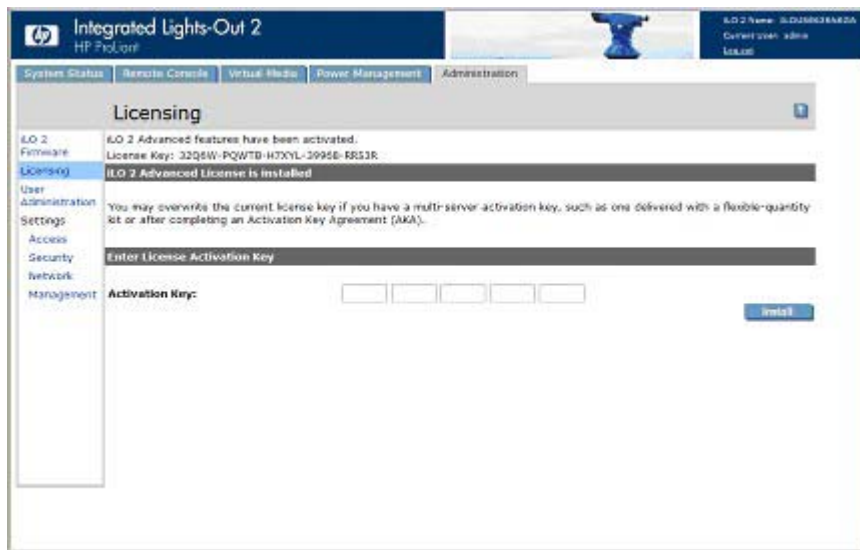
Accedere a iLO 2 da un client di rete remoto utilizzando un browser supportato e fornire il nome DNS, il nome utente e la password predefiniti. Le informazioni sull'account e sul nome DNS predefiniti sono disponibili sull'etichetta delle impostazioni di rete, presente sul server in cui si trova il processore di gestione iLO 2.

Dopo aver eseguito correttamente l'accesso a iLO 2, è possibile modificare i valori predefiniti relativi agli account utente locali selezionando User Administration (Amministrazione utenti) nella scheda iLO 2 Administration (Amministrazione di iLO 2).

Attivazione mediante browser delle funzionalità di iLO 2 per cui è necessaria la licenza

La pagina relativa alle licenze consente di visualizzare lo stato corrente della licenza e di immettere la chiave di attivazione delle funzionalità di iLO 2 che richiedono una licenza. In questa sezione vengono visualizzate la versione di iLO 2 e le informazioni relative alla licenza. Se è installata una versione con licenza (anche se di valutazione), viene visualizzato il relativo numero di licenza. Per ulteriori informazioni sulle opzioni di licenza di iLO 2, vedere la sezione "Licenze" (Licenze a pagina 20).

1. Accedere a iLO 2 tramite un browser supportato.

2. Fare clic su **Administration>Licensing** (Amministrazione>Gestione licenze) per visualizzare la schermata di attivazione della licenza iLO 2.

3. Immettere la chiave di licenza. Per spostarsi tra i diversi campi, premere il tasto **Tab** o fare clic all'interno di un campo. Il campo Activation Key (Chiave di attivazione) viene completato automaticamente dopo l'immissione dei primi caratteri. Fare clic su **Licensing** (Gestione licenze) per cancellare i valori presenti nei campi e ricaricare la pagina.

4. Fare clic su **Installa**. Viene visualizzata la conferma del contratto di licenza con l'utente finale (EULA). I dettagli del contratto sono disponibili sul sito Web HP (http://www.hp.com/servers/lights-out) e nel kit di licenza.

5. Fare clic su **OK**.

Le funzionalità avanzate di iLO risultano abilitate.

Installazione dei driver di iLO 2

iLO 2 Management Interface Driver consente ai componenti software del sistema, quali SNMP Insight Agents e il servizio pass-through di Servizi terminal, di comunicare con iLO 2.

I driver necessari per il supporto di iLO 2 sono contenuti nel pacchetto PSP disponibile nel CD di SmartStart, nel CD di gestione o nel sito Web HP (http://www.hp.com/servers/lights-out).

Per scaricare i driver di supporto per il server e per iLO 2, visitare il sito Web HP (http://www.hp.com/servers/lights-out).

Per scaricare i driver:

1. Fare clic sull'icona iLO 2.

2. Selezionare **Software and Drivers** (Software e driver).

Supporto dei driver Microsoft

I driver dei dispositivi necessari per il supporto di iLO 2 sono contenuti nel pacchetto PSP disponibile nel sito Web HP (http://www.hp.com/support) o sul CD di SmartStart. Prima di installare i driver di Windows®, procurarsi la documentazione di Windows® e la versione più aggiornata di Windows® Service Pack.

File di supporto per iLO 2:

- CPQCIDRV.SYS fornisce il supporto per iLO 2 Management Interface Driver.
- CPQASM2.SYS, SYSMGMT.SYS e SYSDOWN.SYS forniscono il supporto per iLO 2 Advanced Server Management Controller Driver.

PSP per i prodotti Microsoft® Windows® include un programma di installazione che analizza i requisiti di sistema e installa tutti i driver. PSP è disponibile nel sito Web HP (http://www.hp.com/support) o sul CD di SmartStart.

Per installare i driver contenuti nel pacchetto PSP:

1. Scaricare il pacchetto PSP disponibile nel sito Web HP (http://www.hp.com/support).
2. Eseguire il file SETUP.EXE incluso nel pacchetto scaricato e seguire le istruzioni di installazione.

Per ulteriori informazioni sull'installazione di PSP, consultare il file di testo incluso in PSP.

Supporto dei driver Linux

È possibile scaricare i file LSP contenenti il driver di iLO 2, gli agenti Foundation e gli agenti di sicurezza dal sito Web HP all'indirizzo http://www.hp.com/support. Le istruzioni relative all'installazione o all'aggiornamento del driver di iLO 2 sono disponibili nel sito Web. HP Managements Agents per Linux sono i seguenti:

- Il pacchetto ASM (hp-snmp-agents) combina in un solo pacchetto il driver di sicurezza, il visualizzatore IML, gli agenti Foundation, gli agenti di sicurezza e l'agente standard dell'apparecchiatura.
- Il pacchetto RSM (hp-iLO) combina in un solo pacchetto il driver RIB, il daemon del rack, l'agente RIB e l'agente del rack.

Per caricare i pacchetti dei driver di iLO 2 e di sicurezza, eseguire questi comandi:

```
rpm -ivh hp-snmp-agents-d.vv.v-pp.Linux_version.i386.rpm

rpm -ivh hp-iLO-d.vv.v-pp.Linux_version.i386.rpm
```

dove *d* rappresenta la distribuzione e la versione di Linux e

vv.v-pp sono i numeri di versione.

Per ulteriori informazioni, consultare la pagina Software and Drivers (Software e driver) del sito Web HP (http://www.hp.com/support).

Per rimuovere i driver di iLO 2 e di sicurezza, eseguire questi comandi:

```
rpm -e hp-snmp-agents

rpm -e hp-iLO
```

Per ulteriori informazioni, consultare la pagina Software and Drivers (Software e driver) del sito Web HP (http://www.hp.com/support).

Supporto dei driver Novell NetWare

I driver dei dispositivi necessari per il supporto di iLO 2 sono inclusi nel pacchetto PSP, disponibile sul CD di SmartStart e nel sito Web HP (http://www.hp.com/support). PSP per Novell NetWare include un programma di installazione che analizza i requisiti di sistema e installa tutti i driver.

Per iLO 2 sono necessari i seguenti file:

- Il file CPQHLTH.NLM comprende il driver di sicurezza per Novell NetWare.
- Il file CPQCI.NLM fornisce il supporto per iLO 2 Management Interface Driver.

Se si stanno aggiornando i driver di iLO 2, accertarsi che iLO 2 stia eseguendo l'ultima versione del firmware corrispondente. Per ottenere la versione più recente disponibile come componente Smart, visitare il sito Web HP (http://www.hp.com/servers/lights-out).

Per installare i driver, scaricare PSP dal sito Web HP (http://www.hp.com/support) su un server NetWare. Dopo aver scaricato PSP, completare l'installazione seguendo le istruzioni per l'installazione dei componenti NetWare. Per ulteriori informazioni sull'installazione di PSP, consultare il file di testo incluso in PSP.

Con il sistema operativo NetWare 6.X viene fornito un driver video ATI ES1000. Per ottenere i migliori risultati, si consiglia di utilizzare tale driver.

3 Configurazione di iLO 2

In questa sezione

Panoramica sulla configurazione di iLO 2

In genere iLO 2 viene configurato da un utente avanzato o con privilegi amministrativi, responsabile della gestione di altri utenti e della configurazione delle impostazioni globali e di rete. Per configurare iLO 2 è possibile utilizzare l'interfaccia grafica basata su browser o gli strumenti di scripting quali CPQLOCFG e HPONCFG (descritti nella *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*).

Le opzioni disponibili nella scheda Administration (Amministrazione) di iLO 2 consentono di configurare e gestire le impostazioni utente e gli allarmi SNMP (grazie all'integrazione con HP SIM), le impostazioni di protezione, la concessione di licenze, la gestione dei certificati, le impostazioni delle directory e quelle dell'ambiente di rete. Nella scheda Administration (Amministrazione) sono disponibili le seguenti opzioni:

- iLO 2 Firmware (Firmware di iLO 2) (Aggiornamento del firmware di iLO 2 a pagina 17)
- Licensing (Licenze) (Licenze a pagina 20)
- User Administration (Amministrazione utente) (Amministrazione degli utenti a pagina 22)
- Settings (Impostazioni)
  - Access (Accesso) (Configurazione dell'accesso a iLO 2 a pagina 28)
  - Security (Protezione) (Protezione a pagina 38)
  - Network (Rete) (Rete a pagina 61)
  - Management (Gestione) (Impostazioni di SNMP/Insight Manager a pagina 67)

Aggiornamento del firmware di iLO 2

Gli aggiornamenti del firmware consentono di migliorare le funzionalità di iLO 2. La versione più recente del firmware è disponibile sul sito Web HP all'indirizzo http://www.hp.com/servers/lights-out.

Selezionare il prodotto iLO 2, quindi **Software & Drivers** (Software e driver). Una volta visualizzata la pagina relativa al software e ai driver, selezionare il prodotto iLO 2 e il sistema operativo appropriati, quindi fare clic su **Locate Software** (Individua software). È anche possibile individuare il software iLO 2 mediante le opzioni **Operating System** (Sistema operativo) e **Category** (Categoria).

Per aggiornare il firmware è necessario disporre del privilegio Configure iLO (Configura iLO), a meno che non sia impostato l'interruttore di esclusione della protezione (vedere la sezione Amministrazione dell'interruttore di esclusione della protezione di iLO 2 a pagina 40). Se l'interruttore è impostato, il firmware può essere aggiornato da qualsiasi utente di iLO 2. È necessario eseguire gli aggiornamenti del firmware da un contesto di amministratore o radice sul sistema operativo host.

Per aggiornare iLO 2 scegliere uno dei metodi riportati di seguito:

- Aggiornamento del firmware online – Scaricare il componente appropriato per il sistema operativo utilizzato ed eseguirlo nel contesto amministratore o radice del sistema operativo. Il software di aggiornamento del firmware online viene eseguito sul sistema operativo host e aggiorna il firmware di iLO 2 senza che sia necessario accedere a iLO 2.
- Aggiornamento del firmware offline per il CD di manutenzione SmartStart – Scaricare il file con l'immagine del firmware di iLO 2 che si prevede di installare (vedere la sezione "Aggiornamento di iLO 2 mediante un browser" Aggiornamento di iLO 2 mediante un browser a pagina 18).
- CD-ROM di manutenzione del firmware – Scaricare il componente per creare un CD di avvio contenente numerosi aggiornamenti del firmware per le opzioni e i server ProLiant.
- Scripting con CPQLOCFG – Scaricare l'utility di scripting basata su rete CPQLOCFG. CPQLOCFG consente di utilizzare in modo sicuro attraverso la rete gli script RIBCL per l'esecuzione degli aggiornamenti del firmware, la configurazione di iLO 2 e altre operazioni in blocco relative a iLO 2. Gli utenti Linux possono esaminare gli esempi di script in XML e PERL per HP LightsOut.
- Scripting con HPONCFG – Scaricare l'utility di scripting basata su host, HPONCFG. Questa utility consente di utilizzare script RIBCL per l'esecuzione degli aggiornamenti del firmware, la configurazione del processore Lights-Out e di altre operazioni in blocco usando un account che dispone dei privilegi di accesso alla directory principale o dell'amministratore sui sistemi operativi host.
- Utility HP Directories Support for Management Processors – Scaricare l'eseguibile di HP Directories Support for Management Processors nella directory dei componenti di supporto. Uno dei componenti, HPLOMIG, può essere utilizzato per rilevare i processori iLO, iLO 2, RILOE e RILOE II e aggiornare il relativo firmware. Per usufruire di questa funzionalità non è necessario utilizzare l'integrazione delle directory.

Aggiornamento di iLO 2 mediante un browser

È possibile eseguire l'aggiornamento del firmware da qualsiasi client di rete utilizzando un browser supportato. Per aggiornare il firmware di iLO 2 è necessario disporre del privilegio Update iLO 2 Firmware (Aggiorna firmware di iLO 2). La versione più recente del firmware di iLO 2 è disponibile nel sito Web HP (http://www.hp.com/servers/lights-out).

Per aggiornare il firmware di iLO 2 mediante un browser supportato:

1. Accedere a iLO 2 usando un account che dispone del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).

2. Fare clic su **Administration>Upgrade iLO 2 Firmware** (Amministrazione>Aggiorna firmware di iLO 2). Viene visualizzata la pagina Upgrade iLO 2 Firmware (Aggiorna firmware di iLO 2).

3. Immettere il nome file nel campo New firmware image (Nuova immagine firmware) oppure cercare il file.

4. Fare clic su **Send firmware image** (Invia immagine firmware). L'aggiornamento del firmware richiede alcuni minuti. Una barra indica l'avanzamento del processo di aggiornamento.

Non interrompere una sessione di aggiornamento del firmware di iLO 2. Il sistema iLO 2 viene reimpostato automaticamente dopo il completamento di un aggiornamento del firmware. La reimpostazione del sistema iLO 2 non influisce sul server e sul sistema operativo host.

Se l'aggiornamento del firmware viene interrotto, riprovare immediatamente. Non reimpostare il sistema iLO 2 prima di tentare nuovamente l'aggiornamento del firmware.

Aggiornamento del firmware mediante il CD di manutenzione

Per utilizzare HP Smart Update Manager sul CD di manutenzione del firmware:

1. Inserire il CD di manutenzione del firmware su una chiave USB utilizzando USB Key Creator Utility.
2. Copiare il file CP009768.exe nella directory /compaq/swpackages della chiave USB.
3. Seguire le istruzioni di HP Smart Update Manager per completare l'aggiornamento del firmware.

Ripristino di un aggiornamento del firmware di iLO 2 non riuscito

Per ripristinare un aggiornamento del firmware non riuscito mediante l'utility HP Drive Key Boot.

1. Copiare il componente flash non in linea di iLO 2 sulla chiave USB.
2. Verificare che l'interruttore di esclusione della protezione di iLO 2 sia disabilitato.
3. Avviare la chiave USB locale contenente il componente di riprogrammazione di iLO 2

   Per scaricare l'utility HP Drive Key Boot Utility e ottenere informazioni sulla creazione di una chiave USB di avvio, visitare il sito Web HP all'indirizzo http://www.hp.com/go/support.

4. Quando vene visualizzata la prima schermata, passare alla console di testo premendo la combinazione di tasti **Ctrl+Alt+F1**.

5. Spostarsi nella directory in cui è memorizzato il componente flash digitando `cd /mnt/usb/components/` al prompt #.
6. Rimuovere il driver HP Lights-Out corrente immettendo i seguenti comandi:

   `/etc/init.d/hp-snmp-agents stop`

   `/etc/init.d/hp-iLO stop`

   oppure

   `/etc/init.d/hpasm stop`
7. Eseguire il componente mediante l'opzione –direct. Ad esempio:

   `./CP00xxxx.scexe --direct`
8. Al prompt Continue (y/N)? (Continuare (y/N)?), immettere **y**.
9. Dopo aver completato correttamente la programmazione, impostare l'interruttore di esclusione della protezione su **enabled** (abilitato) e riavviare il server.

Downgrade del firmware di iLO 2

Se si esegue il downgrade del firmware di iLO 2, è necessario rimuovere l'applet Remote Console ActiveX 1.3.0.19 di iLO 2 1.30 dal browser client Internet Explorer. Per rimuovere l'applet:

1. Avviare Internet Explorer.
2. Selezionare **Strumenti>Opzioni Internet>Impostazioni>Visualizza oggetti**.
3. Per rimuovere 1.30.19, fare clic con il pulsante destro del mouse su **iLO2 Remote console 1.3.0.18**.

Licenze

Le licenze di HP iLO Advanced Pack e HP iLO Advanced Pack for Blade System attivano funzionalità iLO 2 opzionali non incluse nei sistemi privi di licenza. Per ulteriori informazioni, visitare il sito Web HP.

Acquistando iLO Advanced Pack o iLO Advanced Pack for Blade System con una suite Insight Control o con iLO Power Management Pack, è possibile usufruire dei servizi di aggiornamento e assistenza tecnica HP. Per ulteriori informazioni, vedere "Informazioni di supporto (Informazioni relative al supporto a pagina 240)".

Se si acquista iLO Advanced Pack o iLO Advanced Pack for Blade System per una singola attivazione delle funzionalità che richiedono una licenza, è necessario acquistare gli aggiornamenti successivi. Per ulteriori informazioni, vedere "Informazioni di supporto (Informazioni relative al supporto a pagina 240)".

È necessaria una licenza iLO Advanced o iLO Advanced Pack for Blade System per ogni server su cui il prodotto è installato e utilizzato. Le licenze non sono trasferibili. Non è possibile utilizzare una licenza iLO Advanced for BladeSystem per un server HP ProLiant ML/DL. Per ulteriori informazioni, consultare il Contratto di licenza dell'utente finale (EULA).

HP continua a fornire gratuitamente release di manutenzione con correzioni e miglioramenti alle funzionalità di iLO Standard e iLO Standard Blade Edition.

È possibile scaricare dal sito Web HP una chiave di licenza di valutazione con validità 60 giorni. che consente di attivare e abilitare l'accesso alle funzionalità di iLO 2 Advanced. È possibile installare una sola licenza di valutazione per processore iLO 2. Al termine del periodo di valutazione, le funzionalità di iLO 2 vengono disattivate.

Sono disponibili le seguenti versioni di iLO 2:

NOTA: Le funzionalità contrassegnate con un asterisco (*) non sono supportate su tutti i sistemi.

Funzione	iLO 2 Advanced:	iLO 2 Advanced for Blade System	iLO 2 Standard	iLO 2 Standard Blade Edition
Accensione e Reset virtuale	√	√	√	√
Accesso alla console del server tramite POST	√	√	√	√
Console di testo dopo il POST	√	√	—	—
Registri degli eventi	√	√	√	√
Stato del sistema* e configurazione	√	√	√	√
UID	√	√	√	√
CLP standard SMASH DMTF	√	√	√	√
Script RIBCL/XML	√	√	√	√
Scripting WS-Management	√	√	√	√
Accesso tramite browser	√	√	√	√
Accesso SSH	√	√	√	√
Porta di rete condivisa	√	—	√	—
Accesso seriale	√	√	√	√
Console seriale remota	√	√	√	√
Console remota integrata	√	√	—	√
Console remota	√	√	—	√
Applet Virtual Media	√	√	—	√
Supporto per schede Secure Digital*	√	√	—	√
Pass-through di Servizi terminal	√	√	—	√
Scripting di Virtual Media	√	√	—	—
Integrazione di directory	√	√	—	—
Segnalazioni relative all'alimentazione*	√	√	—	—
Limitazione dell'alimentazione dinamica	√	√	—	—

Funzione	iLO 2 Advanced:	iLO 2 Advanced for Blade System	iLO 2 Standard	iLO 2 Standard Blade Edition
Limitazione dell'alimentazione di gruppo	√	√	—	—
Autenticazione smart card a due fattori	√	√	—	—
HP SIM SSO	√	√	—	—
Debugger del kernel per Windows	√	√	—	—
Riproduzione su console	√	√	—	—
Console remota condivisa	√	√	—	—
Acquisizione sequenze di avvio/errore della console	√	√	—	—
Lettore video iLO (per l'acquisizione è necessaria una licenza)	√	√	√	√

Oltre alle licenze standard di iLO 2 per singolo server, sono disponibili altre due opzioni di licenza:

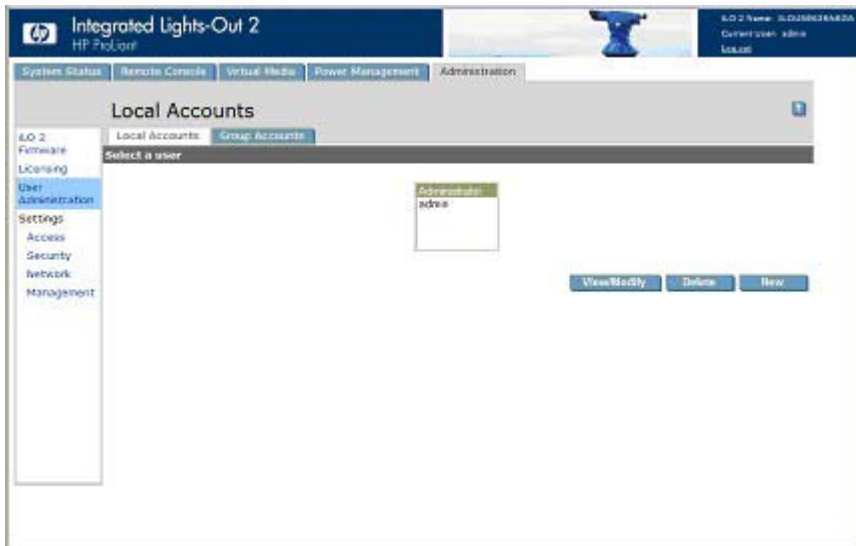
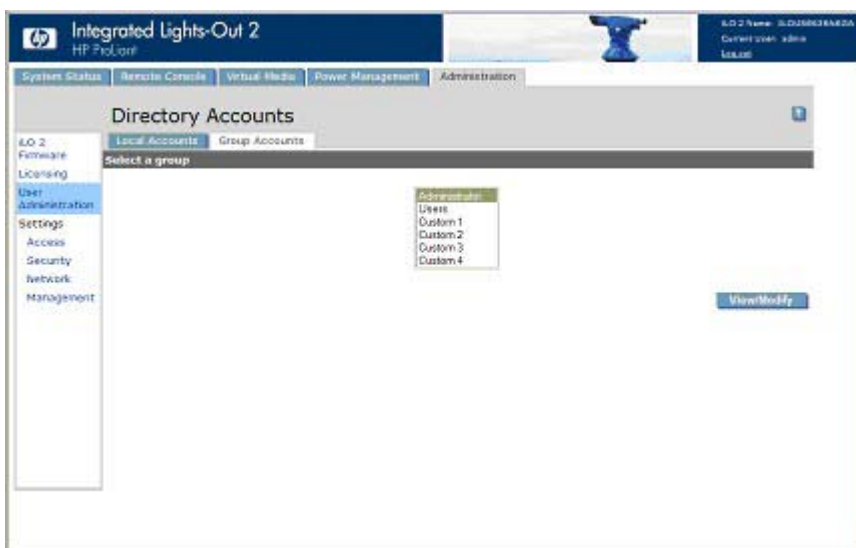
- Il kit Flexible Quantity License consente di acquistare un solo pacchetto software, una copia della documentazione e una sola chiave di licenza per l'attivazione del numero di licenze richiesto.
- L'opzione Activation Key Agreement consente l'acquisto di numerose licenze di ProLiant Essentials e Insight Control nel corso del tempo, generalmente in combinazione con nuovi server ProLiant.

Amministrazione degli utenti

iLO 2 consente di gestire gli account utente salvati localmente nella memoria iLO 2 protetta e gli account dei gruppi di directory. Per gestire gli account utente di directory, utilizzare MMC o ConsoleOne.

iLO 2 supporta fino a 12 utenti con diritti di accesso personalizzabili, nomi di accesso e codifica avanzata della password. Le impostazioni dei singoli utenti sono controllate tramite privilegi. Gli utenti possono disporre di privilegi personalizzati in base a specifici requisiti di accesso. Per il supporto di oltre 12 utenti, è necessario disporre dell'Advanced Pack, che consente l'integrazione con un numero illimitato di account utente basati su directory.

Per visualizzare gli utenti di iLO 2, aggiungerne altri e modificare o eliminare gli utenti esistenti, è necessario disporre del privilegio Administer User Accounts (Amministra account utente). Se non si dispone di questo privilegio, è possibile visualizzare e modificare solo il proprio account.

Per accedere agli account locali, fare clic su **Administration>User Administration>Local Accounts** (Amministrazione>Amministrazione utenti>Account locali).

La schermata Directory Accounts (Account directory) di iLO 2 consente di visualizzare i gruppi di iLO 2 e di modificare le impostazioni per tali gruppi. A tale scopo è necessario disporre del privilegio Administer Directory Groups (Amministra gruppi directory). Per accedere alla schermata Directory Accounts (Account directory), fare clic su **Administration>User Administration>Group Accounts** (Amministrazione>Amministrazione utenti>Account gruppo).

Aggiunta di un nuovo utente

NOTA: Solo gli utenti che dispongono del privilegio Administer User Accounts (Amministra account utente) possono gestire altri utenti su iLO 2.

È possibile assegnare a ogni utente un privilegio di accesso diverso. Ogni utente può disporre di una serie univoca di privilegi specifici per le operazioni che intende eseguire. È possibile concedere o negare l'accesso a funzioni critiche quali l'accesso remoto, la gestione degli utenti, l'accensione virtuale e così via.

Per aggiungere un nuovo utente a iLO 2:

1. Accedere a iLO 2 mediante un account che dispone del privilegio Administer User Accounts (Amministra account utente).
2. Fare clic su **Administration** (Amministrazione).
3. Selezionare **User Administration>Local Accounts** (Amministrazione utenti>Account locali).
4. Fare clic su **New** (Nuovo).

5. Immettere i dati appropriati nei campi. Sono disponibili le opzioni riportate di seguito:
   - Il campo User Name (Nome utente) consente di impostare il nome utente visualizzato nell'elenco degli utenti e sulla home page. Non corrisponde necessariamente al nome di accesso. Il nome utente può avere una lunghezza massima di 39 caratteri e deve includere caratteri stampabili.
   - Il campo Login Name (Nome accesso) consente di impostare il nome da utilizzare per l'accesso a iLO 2. Il nome di accesso può avere una lunghezza massima di 39 caratteri e può includere solo caratteri stampabili.
   - I campi Password e Confirm Password (Conferma password) consentono di impostare e confermare la password utilizzata per l'accesso a iLO 2. È possibile impostare la lunghezza massima per la password nella pagina Access Options (Opzioni di accesso). La password può avere una lunghezza massima di 39 caratteri. Confermare la password immettendola una seconda volta.
   - Administer User Accounts (Amministra account utente) è un privilegio utente che consente di aggiungere, modificare ed eliminare gli account utente iLO 2 locali, nonché di modificare i privilegi di tutti gli utenti, inclusa la concessione delle proprie autorizzazioni. Senza questo privilegio, è possibile visualizzare solo le proprie impostazioni e modificare la propria password.
   - Remote Console Access (Accesso console remota) è un privilegio utente che consente di accedere in remoto alla console seriale remota e alla console remota del sistema host e di controllarne il monitor, la tastiera e il mouse. Per utilizzare questa funzionalità è comunque necessario disporre dell'accesso al sistema remoto.
   - Virtual Power and Reset (Accensione virtuale e reimpostazione) è un privilegio utente che consente di spegnere, accendere o reimpostare la piattaforma host. L'esecuzione di una

qualsiasi di queste attività determina l'interruzione della disponibilità del sistema. È inoltre possibile eseguire la diagnosi del sistema utilizzando il pulsante NMI virtuale.

- Virtual Media (Supporti virtuali) è un privilegio utente che consente di utilizzare supporti virtuali sulla piattaforma host.
- Configure iLO 2 Settings (Configura impostazioni di iLO 2) è un privilegio che consente di configurare la maggior parte delle impostazioni di iLO 2, incluse quelle di protezione. Consente inoltre di aggiornare il firmware di iLO 2 in remoto, ma non include l'amministrazione degli account utente. È raro che queste impostazioni vengano modificate.

  Dopo aver configurato iLO 2 nel modo corretto, revocare a tutti gli utenti questo privilegio per evitare riconfigurazioni successive. Questo privilegio può essere abilitato o disabilitato da un utente che dispone del privilegio Administer User Accounts (Amministra account utente). È inoltre possibile riconfigurare iLO 2 se la relativa utility RBSU è abilitata.
- La sezione User Certificate Information (Informazioni certificato utente) consente di associare un certificato a un utente. I certificati utente sono necessari solo per l'autenticazione basata su due fattori. Se all'account utente non è associato alcun certificato, insieme al pulsante Add a Certificate (Aggiungi certificato) viene visualizzato il messaggio `A certificate has NOT been mapped to this user` (NON è presente alcun certificato associato a questo utente). Fare clic su questo pulsante per associare un certificato all'utente. Dopo l'associazione di un certificato all'account utente, viene visualizzata un'identificazione del certificato composta da 40 cifre, insieme al pulsante Remove this Certificate (Rimuovi certificato), che è possibile utilizzare per rimuovere il certificato. Se Two-Factor Authentication (Autenticazione basata su due fattori) è abilitata, è necessario associare un certificato differente a ciascun utente. Un utente che presenta un certificato al momento della connessione a iLO 2 viene autenticato come utente a cui è associato il certificato. Per l'autenticazione tramite certificato è necessario che Two-Factor Authentication (Autenticazione basata su due fattori) sia abilitata.

6. Una volta completato il profilo utente, fare clic su **Save User Information** (Salva informazioni utente) per tornare alla schermata User Administration (Amministrazione utenti). Per cancellare il profilo utente durante l'aggiunta di un nuovo utente, fare clic su **Restore User Information** (Ripristina informazioni utente).

Visualizzazione o modifica delle impostazioni di un utente

1. Accedere a iLO 2 mediante un account che dispone del privilegio Administer User Accounts (Amministra account utente).

   Per gestire altri utenti su iLO 2 è necessario disporre del privilegio Administer User Accounts (Amministra account utente). Tutti gli utenti possono modificare la propria password mediante la funzionalità View/Modify User (Visualizza/Modifica utente).
2. Fare clic su **Administration>User Administration** (Amministrazione>Amministrazione utente) e selezionare il nome dell'utente di cui si desidera modificare le informazioni.

3. Fare clic su **View/Modify** (Visualizza/Modifica).

4. Modificare le informazioni dell'utente nel modo desiderato.

5. Dopo aver modificato i campi, fare clic su **Save User Information** (Salva informazioni utente) per tornare alla schermata User Administration (Amministrazione utenti). Per recuperare le informazioni originali dell'utente, fare clic su **Restore User Information** (Ripristina informazioni utente). Tutte le modifiche apportate al profilo verranno ignorate.

Eliminazione di un utente

NOTA: Solo gli utenti che dispongono del privilegio Administer User Accounts (Amministra account utente) possono gestire altri utenti su iLO 2.

Per eliminare le informazioni di un utente esistente:

1. Accedere a iLO 2 mediante un account che dispone del privilegio Administer User Accounts (Amministra account utente). Fare clic su **Administration** (Amministrazione).

2. Fare clic su **User Administration** (Amministrazione utenti), quindi selezionare dall'elenco il nome dell'utente di cui si desidera modificare le informazioni.

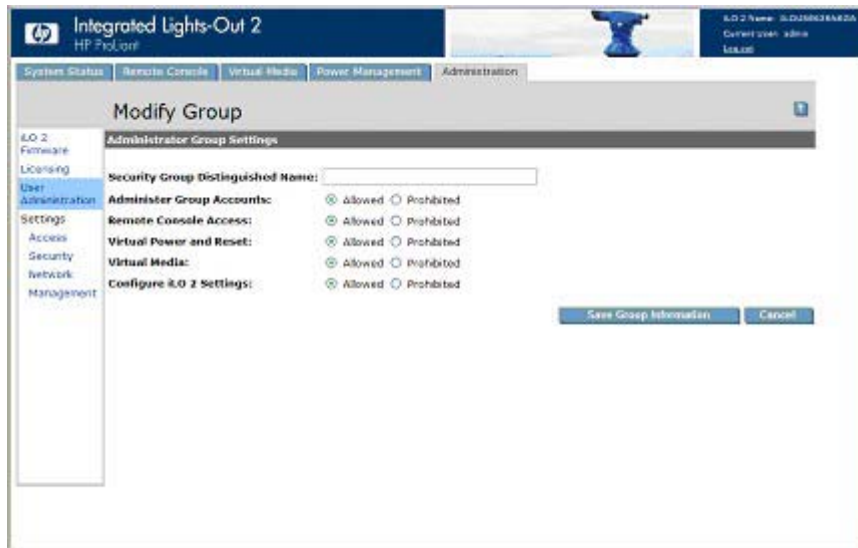
3. Fare clic su **Delete User** (Elimina utente). Viene visualizzato il messaggio `Are you sure you want to delete the selected user?` (Eliminare l'utente selezionato?). Fare clic su **OK**.

Amministrazione dei gruppi

iLO 2 consente di visualizzare i gruppi di iLO 2 e di modificare le relative impostazioni. A tale scopo è necessario disporre del privilegio Administer Directory Groups (Amministra gruppi directory). Per visualizzare o modificare un gruppo:

1. Fare clic su **Administration>User Administration>Group Accounts** (Amministrazione>Amministrazione utenti>Account gruppo).

2. Selezionare il gruppo, quindi fare clic su **View/Modify Group** (Visualizza/Modifica gruppo). Viene visualizzata la pagina Modify Group (Modifica gruppo).

   Fare clic su **Cancel** (Annulla) per tornare alla pagina Group Administration (Amministrazione gruppi).

Sono disponibili le seguenti impostazioni:

- Il campo Security Group Distinguished Name (Nome distinto del gruppo di protezione) consente di impostare il nome distinto di un gruppo all'interno della directory. I privilegi impostati per il gruppo in oggetto vengono assegnati a tutti i membri del gruppo stesso. Il gruppo specificato in Security Group Distinguished Name (Nome distinto del gruppo di protezione) deve essere presente nella directory e gli utenti che richiedono l'accesso a iLO 2 devono essere membri di tale gruppo. In questo campo è necessario immettere un nome distinto della directory, ad esempio CN=Group1,OU=Managed Groups, DC=domain, DC=extension).
- Administer Group Accounts (Amministra account gruppo) consente agli utenti appartenenti al gruppo in oggetto di modificare i privilegi relativi a qualsiasi gruppo.
- Remote Console Access (Accesso console remota) consente di accedere in remoto alla console remota del sistema host, compresa la console seriale remota. Per utilizzare questa funzionalità, è necessario disporre dell'accesso al sistema remoto.
- Virtual Power and Reset (Accensione virtuale e reimpostazione) consente di spegnere, accendere o reimpostare la piattaforma host. Queste attività determinano l'interruzione della disponibilità del sistema. Se questa opzione è selezionata, è possibile anche eseguire la diagnosi del sistema utilizzando il pulsante NMI virtuale.
- Virtual Media (Supporti virtuali) consente di utilizzare supporti virtuali sulla piattaforma host.
- Configure iLO 2 Settings (Configura impostazioni di iLO 2) consente di configurare la maggior parte delle impostazioni di iLO 2, incluse quelle di protezione. Se questa opzione è selezionata, è possibile aggiornare in remoto il firmware di iLO 2. Non è inclusa l'amministrazione degli account di gruppo. È raro che queste impostazioni vengano modificate.

  Dopo aver configurato iLO 2 nel modo corretto, si consiglia di revocare a tutti i gruppi questo privilegio per evitare riconfigurazioni successive. Questo privilegio può essere abilitato o disabilitato dagli utenti che dispongono del privilegio Administer Group Accounts (Amministra account gruppo). È inoltre possibile riconfigurare iLO 2 se la relativa utility RBSU è abilitata.

Fare clic su **Save Group Information** (Salva informazioni gruppo) per salvare le informazioni aggiornate oppure fare clic su **Cancel** (Annulla) per annullare le modifiche e tornare alla pagina Group Administration (Amministrazione gruppi).

Configurazione dell'accesso a iLO 2

iLO 2 consente di configurare i servizi abilitati e l'accesso degli utenti. Per configurare le opzioni dei servizi di iLO 2 (Opzioni dei servizi a pagina 28), fare clic su **Administration>Access** (Amministrazione>Accesso). Viene visualizzata la scheda Services (Servizi). Per configurare le opzioni di accesso a iLO 2 (Opzioni di accesso a pagina 34), fare clic su **Administration>Access>Options** (Amministrazione>Accesso>Opzioni) (scheda). Per modificare le opzioni dei servizi e le opzioni di accesso di iLO 2, è necessario disporre del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).

Opzioni dei servizi

La scheda Services (Servizi) consente di selezionare i servizi da abilitare su iLO 2, inclusi SSH, SSL, la console remota, telnet e Servizi terminal, e di impostare le porte per ogni opzione selezionata. Le impostazioni definite in questa scheda vengono applicate a tutti gli utenti di iLO 2. Per modificarle, è necessario disporre del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).

Per accedere alla scheda Services (Servizi), fare clic su **Administration>Access>Services** (Amministrazione>Accesso>Servizi). Fare clic su **Apply** (Applica) per salvare le informazioni aggiornate. Per rendere effettive le modifiche è necessario riavviare iLO 2. Se sono state apportate modifiche per abilitare o disabilitare la funzionalità di Lights-Out, fare clic su **Apply** (Applica) per interrompere la connessione del browser e riavviare iLO 2. È necessario attendere almeno 30 secondi prima di tentare di ristabilire una connessione.

Nella scheda Services (Servizi) sono disponibili le seguenti impostazioni:

Parametro	Valore predefinito	Descrizione
Secure Shell (SSH) Access (Accesso Secure Shell (SSH))	Abilitato	Questa impostazione consente di specificare se la funzione SSH su iLO 2 è abilitata o disabilitata.
Secure shell (SSH) Port (Porta Secure Shell (SSH))	22	Questa impostazione consente di configurare la porta SSH di iLO 2 da utilizzare per le comunicazioni SSH.
Telnet Access (Accesso Telnet)	Disabilitato	Questa impostazione consente di collegare un client Telnet alla porta Telnet/Console remota, in modo da poter effettuare l'accesso al CLP di iLO 2. È possibile scegliere tra le seguenti opzioni: • Enabled (Abilitato) – iLO 2 consente la connessione dei client Telnet alla porta Telnet/Console remota. Gli scanner della porta di rete sono in grado di rilevare se iLO 2 è in ascolto su questa porta. Sono consentite comunicazioni decodificate tra il CLP di iLO 2 e i client Telnet. • Disabled (Disabilitato) – iLO 2 non consente la connessione dei client Telnet alla porta Telnet/Console remota. Gli scanner della porta di rete non sono in grado di rilevare se la porta è aperta su ILO 2. iLO 2 resterà in ascolto su questa porta per alcuni secondi mentre la porta della console remota viene aperta, ma le connessioni Telnet non verranno accettate. Le comunicazioni tra iLO 2 e la console remota sono sempre codificate.
Remote Console/Telnet Port (Console remota/Porta Telnet)	23	Questa impostazione consente di specificare la porta che iLO 2 dovrà utilizzare per le comunicazioni con la console remota.
Web Server Non-SSL Port (Porta non SSL del server Web)	80	Questa impostazione consente di specificare la porta che il server Web integrato in iLO 2 dovrà utilizzare per le comunicazioni non codificate.
Web Server SSL Port (Porta SSL del server Web)	443	Questa impostazione consente di specificare la porta che il server Web integrato in iLO 2 dovrà utilizzare per le comunicazioni codificate.
Terminal Services Passthrough (Passthrough di Servizi terminal)	Disabilitato	Questa impostazione consente di verificare la capacità di iLO 2 di effettuare il pass-through di una connessione tra un client di Servizi terminal Microsoft® e il server di Servizi terminal in esecuzione

Parametro	Valore predefinito	Descrizione
		sull'host. È possibile scegliere tra le seguenti opzioni: • Automatic (Automatico) – Servizi terminal viene eseguito all'avvio della console remota. • Enabled (Abilitato) – La funzionalità di pass-through viene abilitata e consente di collegare il client di Servizi terminal direttamente a iLO 2 senza effettuare l'accesso. • Disabled (Disabilitato) – La funzionalità di pass-through viene disabilitata.
Terminal Services Port (Porta Servizi terminal)	3389	Questa impostazione consente di configurare la porta di Servizi terminal che iLO 2 dovrà utilizzare per le comunicazioni codificate con il software pass-through di Servizi terminal presente sul server. Se questa porta viene configurata su un valore diverso dall'impostazione predefinita, sarà necessario modificare manualmente il numero della porta.
Virtual Media Port (Porta dei supporti virtuali)	17988	Questa impostazione consente di specificare la porta per il supporto della funzionalità Virtual Media (Supporti virtuali) nelle comunicazioni di iLO 2.
Shared Remote Console Port (Porta console remota condivisa)	9300	Questa impostazione consente di specificare la porta della console remota condivisa. Questa porta viene aperta sul client per consentire ad altri utenti di connettersi alla console remota in modalità peer-to-peer. Questa porta è aperta solo quando la console remota condivisa è in uso.
Console Replay Port (Porta riproduzione console)	17990	Questa impostazione consente di specificare la porta per la riproduzione su console. Questa porta viene aperta sul client per consentire il trasferimento al client dei buffer di cattura interni per la riproduzione. Questa porta è aperta solo quando viene trasferito un buffer di cattura al client.
Raw Serial Data Port (Porta dati seriale Raw)	3002	Questa impostazione consente di specificare l'indirizzo della porta per i dati seriali raw. Questa porta viene aperta solo quando si utilizza l'utility WiLODbg.exe per eseguire il debug in remoto del server host.

Opzione Terminal Services Passthrough

Servizi terminal è disponibile nei sistemi operativi Microsoft® Windows®. L'opzione Terminal Services Passthrough (Pass-through di Servizi terminal) per iLO 2 fornisce una connessione tra il server di Servizi

terminal sul sistema host e il client di Servizi terminal sul sistema client. Quando questa opzione è abilitata, il firmware di iLO 2 abilita un socket che, per impostazione predefinita, rimane in ascolto sulla porta 3389. Tutti i dati ricevuti da Servizi terminal su questa porta vengono inoltrati al server mentre tutti i dati ricevuti dal server vengono inoltrati al socket. Il firmware di iLO 2 legge qualsiasi dato ricevuto su questa porta come pacchetto RDP. I pacchetti RDP vengono scambiati tra il firmware di iLO 2 e il server di Servizi terminal (RDP) attraverso l'indirizzo dell'host locale sul server. Il servizio fornito facilita le comunicazioni tra il firmware di iLO 2 e il server RDP. Il server RDP interpreta il servizio come connessione RDP esterna. Per ulteriori informazioni sul servizio RDP, vedere la sezione "Servizio pass-through RDP di Windows" (Servizio pass-through RDP di Windows a pagina 31).

Una sessione Servizi terminal fornisce una vista migliore, in termini di prestazioni, della console del sistema host. Quando il sistema operativo non è disponibile (oppure il client o il server di Servizi terminal non è disponibile), la console remota tradizionale di iLO 2 fornisce la vista della console del sistema host. Per ulteriori informazioni sulla console remota e su Servizi terminal, vedere la sezione "Client della console remota e di Servizi terminal" (Client della console remota e di Servizi terminal a pagina 33).

Per configurare l'opzione Terminal Services Passthrough (Pass-through di Servizi terminal), vedere le sezioni "Requisiti del client di Servizi terminal" (Requisiti del client di Servizi terminal a pagina 31) e "Installazione del servizio pass-through di Servizi Terminal" (Installazione di pass-through di Servizi Terminal a pagina 32).

Requisiti del client di Servizi terminal

Il client di Servizi terminal è disponibile su client Microsoft® Windows® su cui viene eseguito:

- Windows Server® 2003

  Sui server Windows Server® 2003, il client di Servizi terminal e la connessione RDP sono integrati. Il client fa parte del sistema operativo e viene attivato mediante la condivisione di Desktop remoto. Per attivare la condivisione del desktop, selezionare **Risorse del computer>Proprietà>Remoto>Desktop remoto**. Il client di Servizi terminal fornito con Windows Server® 2003 fornisce opzioni della riga di comando e consente l'avvio di applicazioni senza interruzioni dall'applet della console remota.

- Windows Server® 2008

  Sui server Windows Server® 2008, il client di Servizi terminal e la connessione RDP sono integrati. Il client fa parte del sistema operativo e viene attivato mediante la condivisione di Desktop remoto. Per attivare la condivisione del desktop, selezionare **Risorse del computer>Proprietà>Remoto>Desktop remoto**. Il client di Servizi terminal fornito con Windows Server® 2008 fornisce opzioni della riga di comando e consente l'avvio di applicazioni senza interruzioni dall'applet della console remota.

- Windows® XP

  Sui server Windows® XP, il client di Servizi terminal e la connessione RDP sono integrati. Il client fa parte del sistema operativo e viene attivato mediante la condivisione di Desktop remoto. Per attivare la condivisione del desktop, selezionare **Start>Tutti i programmi>Accessori>Comunicazioni>Desktop remoto**. Il client di Servizi terminal fornito con Windows® XP fornisce opzioni della riga di comando e consente l'avvio di applicazioni senza interruzioni dall'applet della console remota.

Servizio pass-through RDP di Windows

Per utilizzare la funzionalità Terminal Services Passthrough (Pass-through di Servizi terminal) per iLO 2, è necessario installare un servizio pass-through sul sistema host. Questo servizio visualizza il nome del proxy iLO 2 nell'elenco dei servizi disponibili dell'host. Il servizio sfrutta le caratteristiche di protezione e affidabilità di Microsoft® .NET Framework. Dopo l'avvio, il servizio esegue il polling di iLO 2 per determinare se è stata stabilita una connessione RDP con il client. In caso affermativo, il servizio

stabilisce una connessione TCP con l'host locale e inizia lo scambio dei pacchetti. La porta utilizzata per le comunicazioni con l'host locale viene letta dal registro di sistema di Windows® nel seguente percorso:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\Wds
\rdpwd\Tds\tcp\PortNumber
```

In genere si tratta della porta 3389.

Installazione di pass-through di Servizi Terminal

Nella sezione seguente viene descritta la procedura di installazione del servizio pass-through di Servizi terminal in Windows Server® 2008, Windows Server® 2003 e Microsoft® Windows® XP.

- Windows Server® 2003 e Windows Server® 2008

  Per il supporto di Servizi terminal per iLO 2 è necessario che sui server Windows® sia installato Microsoft® .NET Framework. Inoltre, sul server con iLO 2 devono essere installati il servizio pass-through di Servizi terminal e iLO 2 Management Interface Driver per Windows® 2008 e Windows Server® 2003.

  a. Installare iLO 2 Management Interface Driver.

  b. Installare il servizio pass-through avviando il programma di installazione del componente e seguendo le istruzioni fornite nella procedura di installazione guidata.

  Se il servizio è già installato, è necessario riavviarlo manualmente oppure riavviare il server in cui è installato il driver.

  c. Attivare il client di Terminal Services.

  In Windows Server® 2003 e Windows Server® 2008 è possibile attivare la condivisione di Desktop remoto selezionando la scheda **Remoto** in Risorse del computer e scegliendo Proprietà.

  Se l'installazione di iLO 2 è completata e l'opzione Terminal Services Pass-through (Pass-through di Servizi terminal) di iLO 2 è impostata su Automatic (Automatica), Servizi terminal verrà avviato al termine dell'installazione.

- Microsoft® Windows® XP

  In Windows® XP la connessione desktop remoto è integrata e non richiede altre operazioni di installazione.

Gli errori che si verificano durante l'installazione e l'esecuzione del servizio pass-through vengono riportati nel registro eventi dell'applicazione sul server. È possibile rimuovere il servizio pass-through mediante la funzione Installazione applicazioni del Pannello di controllo.

Abilitazione del servizio pass-through di Servizi terminal

Per impostazione predefinita, il servizio pass-through di Servizi terminal è disabilitato. È tuttavia possibile abilitarlo utilizzando la pagina Administration>Access>Services (Amministrazione>Accesso>Servizi). Il pulsante Terminal Services (Servizi terminal) della console remota risulta disattivato finché la funzione pass-through di Servizi terminal non viene abilitata.

L'uso della funzione pass-through di Servizi terminal richiede l'installazione nel server dell'ultima versione di LightsOut Management Interface Driver e della funzione pass-through di Servizi terminal per Microsoft® Windows®.

Quando l'opzione Terminal Services Passthrough (Pass-through di Servizi terminal) è impostata su Enabled (Abilitato) o Automatic (Automatico) nella pagina Administration>Access>Services

(Amministrazione>Accesso>Servizi) e il client di Servizi terminal è installato nel client Windows® (installazione eseguita in modo predefinito con Windows® XP), il pulsante di Servizi terminal è abilitato. Facendo clic sul pulsante di Servizi terminal, l'applet tenta di avviare Servizi terminal, anche se il server non esegue un sistema operativo Windows®.

Confermare i requisiti di licenza Microsoft®, che sono uguali a quelli del collegamento tramite il controller di rete del server. Ad esempio, se si imposta l'accesso di amministratore, Servizi terminal non consentirà di definire più di due connessioni, indipendentemente dal fatto che avvengano tramite il controller di rete del server, tramite iLO 2 o entrambi.

Messaggio di avviso di Servizi terminal

Gli utenti di Servizi terminal che utilizzano Windows® 2003 Server potrebbero rilevare la condizione descritta di seguito durante l'uso della funzione pass-through di Servizi terminal di iLO 2. Se si avvia una sessione di Servizi terminal tramite iLO 2 e l'amministratore di Windows® avvia una seconda sessione di Servizi terminal (in modalità console), la prima sessione di Servizi terminal viene disconnessa. La prima sessione, tuttavia, riceve il messaggio di avviso che informa della disconnessione solo circa un minuto dopo. Durante questo periodo di tempo, la prima sessione di Servizi terminal è disponibile o attiva. Questo comportamento è normale, tuttavia è diverso da quanto si verifica quando entrambe le sessioni di Servizi terminal sono stabilite da amministratori Windows∃. In questo caso, la prima sessione di Servizi terminal riceve immediatamente il messaggio di avviso.

Visualizzazione dell'opzione Terminal Services Passthrough

È possibile che nel firmware di iLO 2 l'opzione Terminal Services Passthrough (Pass-through di Servizi terminal) non venga visualizzata correttamente. Ad esempio, questa opzione può risultare attiva anche se il sistema operativo non è abilitato per Servizi terminal, come nel caso di un sistema operativo host Linux, in cui Servizi terminal non è supportato.

Client della console remota e di Servizi terminal

Utilizzando la connessione della rete di gestione a iLO 2, è possibile servirsi di una sessione della console remota di iLO 2 per visualizzare una sessione di Servizi terminal sull'host. Quando si esegue l'applet della console remota di iLO 2, essa avvia il client di Servizi terminal in base alle preferenze dell'utente. Per disporre della completa funzionalità di questa funzione, è necessario installare JVM Sun. Se JVM Sun non è installato, la console remota non sarà in grado di avviare automaticamente il client di Servizi terminal.

Se la funzione pass-through di Servizi terminal è abilitata e il server di Servizi terminal è disponibile, la commutazione tra la console remota di iLO 2 e il client di Servizi terminal avviene senza interruzioni durante il passaggio del server dall'ambiente del sistema operativo precedente all'ambiente di sistema operativo in esecuzione e successivamente all'ambiente di sistema operativo non disponibile. Il funzionamento senza interruzioni è disponibile finché il client di Servizi terminal non viene avviato prima che sia disponibile la console remota. Se la console remota è disponibile così come il client di Servizi terminal, la console remota avvierà il client di Servizi terminal nel momento appropriato.

Quando si utilizza l'opzione pass-through di Servizi terminal con Windows Server® 2003 e Windows Server® 2008, si verifica un ritardo di circa 30 secondi dopo la visualizzazione della finestra di dialogo CTRL-ALT-CANC prima dell'avvio del client di Servizi terminal. Questo ritardo di 30 secondi rappresenta il periodo di tempo richiesto dal servizio per il collegamento al client RDP in esecuzione sul server. Se il server viene riavviato dal client di Servizi terminal, lo schermo della console remota diventerà grigio o nero per un periodo massimo di un minuto, durante il quale iLO 2 determina la non disponibilità del server di Servizi terminal.

Se la modalità di Servizi terminal è impostata su Enabled (Abilitato) ma si desidera utilizzare la console remota, avviare il client di Servizi terminal direttamente dal relativo menu. Se si avvia direttamente dal

menu del client, è possibile utilizzare contemporaneamente il client di Servizi terminal e la console remota.

Servizi terminal può essere disabilitato o abilitato in qualunque momento. La modifica della configurazione di Servizi terminal causerà la reimpostazione del firmware di iLO 2. La reimpostazione del firmware di iLO 2 determina l'interruzione di qualsiasi connessione aperta con iLO 2.

Quando il client di Servizi terminal viene avviato dalla console remota, questa entra in modalità di sospensione per evitare di utilizzare l'ampiezza di banda della CPU. La console remota rimane in ascolto degli eventuali comandi inviati da iLO 2 sulla porta 23 predefinita della console remota.

iLO 2 esegue il pass-through di una sola connessione di Servizi terminal alla volta. Per Servizi terminal non sono consentite più di due sessioni simultanee.

La console remota risulterà attiva e disponibile nel caso in cui si trovi in modalità di sospensione e il client di Servizi terminal venga interrotto in seguito ai seguenti eventi:

- Chiusura di Servizi terminal da parte dell'utente.
- Arresto del sistema operativo Windows®.
- Blocco del sistema operativo Windows®.

Risoluzione dei problemi di Servizi terminal

Per risolvere i problemi relativi all'opzione pass-through di Servizi terminal di iLO 2:

1. Accertarsi che Servizi terminal sia abilitato sull'host selezionando **Risorse del computer>Proprietà>Remoto>Desktop remoto**.
2. Verificare che la configurazione pass-through di iLO 2 sia abilitata o automatica controllando le impostazioni globali di iLO 2.
3. Accertarsi di disporre della licenza per iLO Advanced Pack.
4. Verificare che iLO 2 Management Interface Driver sia installato nell'host. Per effettuare questa verifica, selezionare **Risorse del computer>Proprietà>Hardware>Gestione periferiche>Schede multifunzionali**.
5. Verificare che il servizio pass-through di Servizi terminal e il proxy iLO 2 siano installati e in esecuzione sull'host. Per effettuare questa verifica, selezionare **Pannello di controllo>Strumenti di amministrazione>Servizi** e tentare di riavviare il servizio.
6. Verificare che il registro eventi dell'applicazione non sia pieno.

   Se il registro eventi dell'applicazione del sistema operativo è pieno, la funzione pass-through di Servizi terminal può avere problemi di avvio. Per visualizzare il registro eventi, selezionare **Gestione computer>Utilità di sistema>Visualizzatore eventi>Applicazione**.
7. Verificare che la porta di Servizi terminal assegnata sia corretta.
8. Verificare che il client di Servizi terminal, `mstsc.exe`, si trovi nel percorso `\WINDOWS\SYSTEM32`.

   In caso contrario, impostare la configurazione pass-through su **Enabled** (Abilitato) e attivare manualmente il client di Servizi terminal.

Opzioni di accesso

È possibile modificare le impostazioni di accesso a iLO 2, inclusi il tempo di inattività della connessione, la funzionalità di iLO 2, l'utility RBSU di iLO 2, i requisiti di accesso, i parametri CLI, la lunghezza minima della password e il nome del server. Le impostazioni definite nella scheda Access Options (Opzioni di

accesso) vengono applicate a tutti gli utenti di iLO 2. Per modificarle, è necessario disporre del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).

Per visualizzare o modificare l'accesso a iLO 2, fare clic su **Administration>Access>Options** (Amministrazione>Accesso>Opzioni) quindi fare clic su **Apply** (Applica) per salvare le informazioni aggiornate. Per rendere effettivi gli aggiornamenti è necessario riavviare iLO 2. Se sono state apportate modifiche per abilitare o disabilitare la funzionalità di Lights-Out, fare clic su **Apply** (Applica) per interrompere la connessione del browser e riavviare iLO 2. È necessario attendere almeno 30 secondi prima di tentare di ristabilire una connessione.

Nella scheda Access Options (Opzioni di accesso) sono disponibili le seguenti impostazioni:

Parametro	Valore predefinito	Descrizioni
Idle Connection Timeout (minutes) (Timeout di connessione inattiva - minuti)	30 minuti	Questa impostazione consente di specificare l'intervallo di inattività dell'utente in minuti prima che la sessione della console remota e del server Web vengano automaticamente terminate. È possibile scegliere tra le seguenti opzioni: 15, 30, 60, 120 minuti o 0 (infinito). Il valore di timeout infinito non determina la disconnessione degli utenti inattivi.
Lights-Out Functionality (Funzionalità Lights-Out)	Abilitato	Questa impostazione consente di abilitare la connessione a iLO 2. Se è disabilitata, tutte le connessioni a iLO 2 vengono negate. Se si disabilita la funzionalità di Lights-Out, la rete iLO 2 da 10/100 MB/s e le comunicazioni con i driver del sistema operativo vengono disabilitate. Viene inoltre disabilitata la porta di diagnostica di iLO 2 per server HP ProLiant BL p-Class.

Parametro	Valore predefinito	Descrizioni
		Se la funzionalità di iLO 2 è disabilitata (inclusa la porta di diagnostica), è necessario utilizzare l'interruttore di esclusione della protezione del server per abilitare iLO 2. Consultare la documentazione del server per individuare l'interruttore di esclusione della protezione e impostarlo per l'esclusione. Accendere il server e utilizzare l'utility RBSU di iLO 2 per impostare Lights-Out Functionality (Funzionalità Lights-Out) su Enabled (Abilitato).
iLO 2 ROM-Based Setup Utility (Utility di configurazione basata sulla ROM iLO 2)	Abilitato	Questa impostazione abilita o disabilita l'utility RBSU (ROM-Based Setup Utility) di iLO 2. In genere, il codice della ROM opzionale di iLO2 chiede di premere **F8** per accedere all'utility RBSU, ma se iLO 2 o la relativa utility RBSU sono disabilitati, il prompt di RBSU viene ignorato.
Require login for iLO 2 RBSU (Richiedi accesso per RBSU di iLO 2)	Disabilitato	Questa impostazione consente l'accesso RBSU, con o senza verifica delle credenziali dell'utente. Se questa impostazione è abilitata e si preme **F8** durante il POST per accedere all'utility RBSU di iLO 2, viene visualizzata una finestra di dialogo di accesso.
Show iLO 2 during POST (Mostra iLO 2 durante il POST)	Disabilitato	Questa impostazione consente di visualizzare l'indirizzo IP di rete di iLO 2 durante il POST del server host.
Serial Command Line Interface Status (Stato interfaccia riga di comando seriale)	Enabled – authentication required (Abilitato – autenticazione necessaria)	Questa impostazione consente di modificare il modello di accesso della funzione CLI tramite la porta seriale. È possibile scegliere tra le seguenti opzioni: • Enabled – Authentication Required (Abilitato – autenticazione necessaria) • Enabled – No Authentication (Abilitato – nessuna autenticazione) • Disabilitato
Serial Command Line Interface Speed (Velocità interfaccia riga di comando seriale della riga di comando)	9600	Questa impostazione consente di utilizzare la porta seriale per modificare la velocità della porta seriale per la funzionalità CLI. I valori di velocità (in bit/ secondo) validi sono 9600, 19200, 38400, 57600 e 115200. La porta seriale deve essere impostata su No parity (Nessuna parità), 8 bit di dati e 1 bit di stop (N/8/1) per il corretto funzionamento. La velocità della porta seriale impostata mediante questo parametro deve corrispondere alla

Parametro	Valore predefinito	Descrizioni
		velocità della porta seriale impostata nell'utility RBSU.
Minimum Password Length (Lunghezza minima password)	8	Questa impostazione consente di specificare il numero minimo di caratteri consentiti per l'impostazione o la modifica di una password utente. La lunghezza dei caratteri deve essere impostata su un valore compreso tra 0 e 39.
Server Name (Nome server)	—	Questa impostazione consente di specificare il nome del server host. Questo valore viene assegnato se si utilizzano gli agenti HP ProLiant Management. Se non si utilizzano gli agenti e viene visualizzato un messaggio relativo all'host senza nome, non è possibile assegnare un nome al server host. Se gli agenti sono in esecuzione, il nome assegnato può essere sovrascritto. Per imporre l'aggiornamento del browser, salvare questa impostazione e premere il tasto **F5**.
Authentication Failure Logging (Registrazione errori autenticazione)	Enabled-Every 3rd Failure (Abilitato-Ogni 3 errori)	Questa impostazione consente di configurare i criteri di registrazione per le autenticazioni non riuscite. Sono supportati tutti i tipi di accesso e ognuno di essi funziona in maniera indipendente. È possibile scegliere tra le seguenti opzioni: • Enabled-Every Failure (Abilitato-Tutti gli errori) – Viene registrata una voce per ogni tentativo di accesso non riuscito. • Enabled-Every 2nd Failure (Abilitato-Ogni 2 errori) – Viene registrata una voce ogni due tentativi di accesso non riusciti. • Enabled-Every 3rd Failure (Abilitato-Ogni 3 errori) – Viene registrata una voce ogni tre tentativi di accesso non riusciti. • Enabled-Every 5th Failure (Abilitato-Ogni 5 errori) – Viene registrata una voce ogni cinque tentativi di accesso non riusciti. • Disabled (Disabilitato) – Non viene registrato alcun tentativo di accesso non riuscito.

Quando si accede a iLO 2 mediante client Telnet o SSH, il numero delle richieste di password e nome di accesso visualizzate da iLO 2 corrisponde al valore del parametro Authentication Failure Logging (Registrazione errori autenticazione) oppure a 3, quando questo è disabilitato. Tuttavia, questo numero

può dipendere anche dalle configurazioni dei client Telnet e SSH. Gli accessi Telnet e SSH implementano anche ritardi dopo un errore di accesso. Durante il ritardo, l'accesso viene disabilitato e quindi non si verifica alcun errore di accesso. Di seguito è riportato un esempio relativo alla generazione di un registro di errori di autenticazione SSH con un valore predefinito quale Enabled-Every 3rd Failure (Abilitato-Ogni 3 errori). Si supponga che si verifichino tre errori di accesso consecutivi nel modo seguente (purché il client SSH sia configurato con un numero di richieste di password >= 3):

1. Esecuzione del client SSH e tentativo di accesso con nome e password non corretti. Vengono visualizzate tre richieste di password. Dopo l'immissione di tre password non corrette, la connessione viene terminata e viene registrato il primo tentativo di accesso non riuscito. Il contatore degli errori di accesso SSH viene impostato su 1.
2. Esecuzione del client SSH fino alla visualizzazione della richiesta di accesso. Tentativo di accesso con nome e password non corretti. Vengono visualizzate tre richieste di password. Dopo l'immissione di tre password non corrette, la connessione viene terminata e viene registrato il secondo tentativo di accesso non riuscito. Il contatore degli errori di accesso SSH viene impostato su 2.
3. Esecuzione del client SSH fino alla visualizzazione della richiesta di accesso. Tentativo di accesso con nome e password non corretti. Vengono visualizzate tre richieste di password. Dopo l'immissione di tre password non corrette, la connessione viene terminata e viene registrato il terzo tentativo di accesso non riuscito. Il contatore degli errori di accesso SSH viene impostato su 3.

A questo punto, il firmware di iLO 2 registra una voce di errore di accesso SSH e reimposta il contatore degli errori di accesso SSH su 0.

Accesso alla console seriale remota e alla console remota di iLO 2

Per le impostazioni client e server consigliate per la console remota di iLO 2, l'ottimizzazione del supporto del mouse e le impostazioni della console seriale remota, vedere la sezione "Console remota di iLO 2" (Console remota di iLO 2 a pagina 86).

Protezione

iLO 2 consente di personalizzare le impostazioni di protezione. Per accedere a queste impostazioni, selezionare **Administration>Security** (Amministrazione>Protezione). Sono disponibili le seguenti opzioni di protezione di iLO 2:

- Amministrazione delle chiavi SSH (Amministrazione delle chiavi SSH a pagina 42)
- Amministrazione dei certificati SSL (Amministrazione dei certificati SSL a pagina 43)
- Autenticazione basata su due fattori (Autenticazione basata su due fattori a pagina 44)
- Impostazioni di directory (Impostazioni di directory a pagina 50)
- Codifica iLO 2
- HP SIM SSO (HP SIM SSO a pagina 56)
- Blocco del computer da console remota (Blocco del computer da console remota a pagina 59)

Le opzioni di protezione consentono a iLO 2 di fornire le seguenti funzionalità:

- Porte TCP/IP definite dall'utente
- Registrazione delle azioni degli utenti nel registro eventi di iLO 2
- Ritardi progressivi per tentativi di accesso non riusciti
- Supporto dei certificati firmati dell'autorità di certificazione X.509

- Supporto per la protezione dell'utility RBSU
- Comunicazioni codificate tramite:
  - Amministrazione delle chiavi SSH
  - Amministrazione dei certificati SSL
- Supporto per servizi di directory basati su LDAP opzionali

Alcune di queste opzioni corrispondono a funzionalità per le quali è necessaria una licenza. Per verificare le opzioni disponibili, vedere la sezione "Licenze" (Licenze a pagina 20).

Istruzioni generali sulla protezione

L'elenco che segue riguarda le istruzioni generali inerenti alla protezione di iLO 2:

- Per ottenere i massimi livelli di protezione, installare iLO 2 su una rete di gestione separata.
- Non collegare iLO 2 direttamente a Internet.
- Utilizzare un browser con livello di codifica a 128 bit.

Istruzioni generali sulle password

Di seguito è riportato un elenco delle istruzioni generali sulle password. È necessario che le password:

- Non vengano scritte o registrate.
- Non vengano comunicate ad altre persone.
- Non contengano parole facili da indovinare, quali il nome dell'azienda, i nomi di prodotto, il nome dell'utente o l'ID utente.
- Includano almeno tre o quattro delle caratteristiche riportate di seguito:
  - Almeno un carattere numerico
  - Almeno un carattere speciale
  - Almeno un carattere minuscolo
  - Almeno un carattere maiuscolo

Gli stessi standard dovranno essere adottati per le password emesse per un ID utente temporaneo, la reimpostazione delle password o un ID utente bloccato. La lunghezza minima delle password può variare da 0 a 39 caratteri. La lunghezza minima predefinita è 8 caratteri. L'impostazione della lunghezza minima delle password su un numero inferiore a 8 non è consigliabile, a meno che non si disponga di una rete di gestione protetta fisicamente che non consenta la propagazione esterna del centro dati protetto.

Protezione di RBSU

L'utility RBSU consente di visualizzare e modificare la configurazione di iLO 2. Le impostazioni di accesso a RBSU possono essere configurate mediante l'utility stessa, un browser Web (vedere la

sezione "Opzioni di accesso" (Opzioni di accesso a pagina 34), script RIBCL oppure l'interruttore di esclusione della protezione di iLO 2. RBSU ha tre livelli di protezione:

- RBSU Login Not Required (Nome di accesso RBSU non richiesto), impostazione predefinita.

  Chiunque disponga dei diritti di accesso all'host durante l'esecuzione del POST può accedere all'utility RBSU di iLO 2 per visualizzare e modificare le impostazioni di configurazione. Questa impostazione è accettabile se l'accesso host è controllato.

- RBSU Login Required (Richiesto nome di accesso RBSU), sicurezza intermedia.

  Se è richiesto il nome di collegamento per RBSU, i menu di configurazione attiva sono gestiti in base ai diritti di accesso concessi agli utenti autenticati.

- RBSU Disabled (RBSU disabilitata), la più sicura.

  Se l'utility RBSU di iLO 2 è disabilitata, l'accesso degli utenti è proibito. In tal modo non è possibile eseguire modifiche tramite l'interfaccia RBSU.

Amministrazione dell'interruttore di esclusione della protezione di iLO 2

Tramite l'interruttore di esclusione della protezione di iLO 2, l'amministratore ha accesso completo al processore iLO 2. Questo accesso può essere necessario in presenza di una delle seguenti condizioni:

- iLO 2 deve essere nuovamente abilitato dopo essere stato disabilitato.
- Tutti gli account utente con il privilegio Administer User Accounts (Amministrazione account utente) sono stati bloccati.
- Errata configurazione con mancata visualizzazione di iLO 2 in rete e disabilitazione dell'utility RBSU.
- Il blocco di avvio deve essere riprogrammato.

L'attivazione della funzione di esclusione della protezione include:

- Disabilitazione di tutti i controlli di autorizzazione sulla protezione durante l'impostazione dell'interruttore.
- Esecuzione dell'utility RBSU di iLO 2 in caso di reimpostazione del server host.
- iLO 2 non è disabilitato e potrebbe essere visualizzato sulla rete come configurato.
- iLO 2, se è disabilitato quando l'interruttore di esclusione della protezione è impostato, non disconnette l'utente e completa il processo di disabilitazione finché il server non viene spento e riacceso.
- Esposizione del blocco di avvio per la programmazione.

Nelle pagine Web di iLO 2 viene visualizzato un messaggio di avviso che indica che l'interruttore di esclusione della protezione è in uso. Nel registro di iLO 2 viene inoltre inserita una voce relativa all'uso dell'interruttore. È anche possibile inviare un allarme SNMP all'attivazione o disattivazione dell'interruttore di esclusione della protezione di iLO 2.

L'attivazione dell'interruttore di esclusione della protezione consente di eseguire l'aggiornamento del blocco di avvio di iLO 2. HP non ritiene che sarà necessario aggiornare il blocco di avvio di iLO 2. Nel caso in cui sia esplicitamente richiesto l'aggiornamento del blocco di avvio di iLO 2, sarà necessario riprogrammare manualmente sul server il blocco di avvio e reimpostare iLO 2. I blocco di avvio rimane esposto fino alla reimpostazione di iLO 2. Per una maggiore protezione, HP consiglia di scollegare iLO 2 dalla rete fino al completamento della reimpostazione. L'interruttore di esclusione della protezione di iLO 2 si trova sul server e non è possibile accedervi senza aprire il contenitore del server.

Per impostare l'interruttore di esclusione della protezioni di iLO 2, procedere come segue:

1. Spegnere il server.
2. Impostare l'interruttore.
3. Accendere il server.

Eseguire la procedura in senso inverso per disattivare l'interruttore di esclusione della protezione di iLO 2.

In base al tipo di server, l'interruttore di esclusione della protezione di iLO 2 può essere costituito da un singolo ponticello o da una posizione specifica dell'interruttore sul pannello dei microinterruttori. Per accedere e individuare l'interruttore, consultare la documentazione del server. Fare inoltre riferimento agli schemi presenti sul pannello di accesso del server.

Supporto Trusted Platform Module

TPM è una funzionalità di protezione del sistema basata sull'hardware. È costituito da un chip per computer in cui è possibile memorizzare in modo protetto alcune informazioni utilizzate per l'autenticazione della piattaforma. Queste informazioni possono includere password, certificati o chiavi di crittografia. Può anche essere utilizzato per memorizzare valori di misurazione della piattaforma che consentono di garantire l'attendibilità della piattaforma. iLO 2 fornisce il supporto per il modulo mezzanine TPM nei server ProLiant 100 e ProLiant 300/500.

In un sistema supportato, iLO 2 decodifica il record TPM e passa lo stato della configurazione all'interfaccia iLO 2, CLP e XML. Nella pagina System Status (Stato sistema) viene visualizzato lo stato della configurazione TPM. Se il sistema host o la ROM di sistema non supporta la funzionalità TPM, nella pagina Status Summary (Riepilogo dello stato) non viene visualizzato lo stato TPM. Nella pagina Status Summary (Riepilogo dello stato) vengono visualizzate le seguenti informazioni relative allo stato TPM:

- Not Present (Non presente) - Il modulo TPM non è installato.
- Present (Presente) - Quando:
  - Il modulo TPM è installato ma disabilitato.
  - Il modulo TPM è installato e abilitato.
  - Il modulo TPM è installato e abilitato ed è abilitata anche la misurazione della ROM di espansione. Se la misurazione della ROM di espansione è abilitata, nella pagina Update iLO 2 Firmware (Aggiorna firmware iLO 2) viene visualizzato un messaggio di avviso legale quando si fa clic su **Send firmware image** (Invia immagine firmware).

Accesso e account utente

iLO 2 consente di configurare fino a 12 account utente locali. Ciascun account può essere gestito tramite le funzioni elencate di seguito:

- Privilegi (Privilegi a pagina 42)
- Protezione dell'accesso (Protezione dell'accesso a pagina 42)

È possibile configurare iLO 2 in modo che utilizzi una directory per autenticare e autorizzare gli utenti. Questa configurazione consente di avere un numero virtualmente illimitato di utenti e di adattarsi agevolmente al numero di dispositivi Lights-Out dell'azienda. La directory, inoltre, costituisce un punto centralizzato per l'amministrazione dei dispositivi e degli utenti Lights-Out e permette un uso più restrittivo delle password. iLO 2 consente di utilizzare utenti locali, utenti di directory o entrambi.

Sono disponibili due opzioni di configurazione: una directory estesa mediante l'apposito schema HP (Impostazione dell'integrazione di directory mediante lo schema HP a pagina 153) o lo schema di directory predefinito (senza schema (Configurazione dell'integrazione di directory senza schema a pagina 149)).

Privilegi

iLO 2 consente all'amministratore di controllare l'accesso degli account utente alle funzioni di iLO 2 attraverso l'uso dei privilegi. Quando un utente tenta di utilizzare una funzione, il sistema iLO 2 verifica che l'utente disponga dei necessari privilegi prima di consentire l'esecuzione della funzione.

Tutte le funzioni disponibili tramite iLO 2 possono essere controllate tramite i privilegi, incluse le funzioni di amministrazione degli account utente, di accesso della console remota, l'accensione virtuale e la reimpostazione, i supporti virtuali e le impostazioni di configurazione di iLO 2. I privilegi per ciascun utente possono essere configurati nella pagina User Administration (Amministrazione utente) della scheda Administration (Amministrazione).

Protezione dell'accesso

iLO 2 fornisce diverse funzioni per la protezione dell'accesso. Dopo un tentativo iniziale di accesso non riuscito, iLO 2 impone un ritardo di cinque secondi. Dopo un secondo tentativo non riuscito, iLO 2 impone un ritardo di 10 secondi. Dopo il terzo tentativo non riuscito, e dopo tutti quelli successivi, iLO 2 impone un ritardo di 60 secondi. Tutti i tentativi di accesso non riusciti successivi torneranno ciclicamente su questi valori. Durante ogni ritardo, viene visualizzata una pagina informativa. Questa sequenza si ripeterà finché non verrà completato un accesso valido. Questa funzione costituisce una protezione contro i cosiddetti attacchi da dizionario contro la porta di accesso del browser.

iLO 2 salva inoltre una voce di registro dettagliata per ciascun tentativo di accesso non riuscito che implica un ritardo di 60 secondi.

Amministrazione delle chiavi SSH

iLO 2 consente di autorizzare contemporaneamente un massimo di quattro chiavi SSH nella scheda SSH Key (Chiave SSH), in cui sono visualizzati anche i proprietari delle chiavi SSH autorizzate (se disponibili). Un solo utente può essere proprietario di più chiavi.

Per aggiungere a iLO 2 una chiave autorizzata, è necessario inoltrare a iLO 2 il percorso della chiave pubblica. In questo file, dopo la chiave deve essere riportato il nome utente. iLO 2 associa ciascuna chiave a un account utente locale. Se l'account utente non esiste o è stato eliminato, la chiave non è valida (se l'account non esiste, la chiave non è inclusa nell'elenco).

In alternativa, è possibile autorizzare le chiavi SSH di un server HP SIM utilizzando lo strumento mxagentconfig dal server HP SIM, specificando l'indirizzo e le credenziali utente per iLO 2. Per informazioni dettagliate, consultare la documentazione relativa a HP SIM.

Per autorizzare una nuova chiave:

1. Nell'interfaccia di iLO 2 fare clic su **Administration>Security>SSH Key** (Amministrazione>Protezione>Chiave SSH).
2. Fare clic su **Browse** (Sfoglia) e individuare il file della chiave.
3. Fare clic su **Authorize Key** (Autorizza chiave).

È possibile visualizzare o eliminare qualsiasi chiave precedentemente autorizzata selezionando la chiave desiderata e facendo clic su **View Selected Key** (Visualizza chiave selezionata) o **Delete Selected Key** (Elimina chiave selezionata). I pulsanti View Selected Key (Visualizza chiave selezionata) e Delete Selected Key (Elimina chiave selezionata) vengono visualizzati solo se sono state installate chiavi SSH.

Amministrazione dei certificati SSL

iLO 2 consente di creare una richiesta di certificato, importare un certificato e visualizzare le informazioni di amministrazione associate a un certificato memorizzato. Le informazioni relative al certificato sono codificate dall'autorità di certificazione e vengono estratte da iLO 2.

Per impostazione predefinita, iLO 2 crea un certificato con autoconvalida da utilizzare nelle connessioni SSL. Con questo certificato, iLO 2 potrà essere utilizzato senza che sia necessario eseguire ulteriori passaggi di configurazione. È possibile migliorare le funzioni di protezione di iLO 2 tramite l'importazione di un certificato attendibile. Per ulteriori informazioni sui certificati e sui relativi servizi, vedere "Introduzione a Servizi certificati" (Introduzione a Servizi certificati a pagina 149) e "Installazione di Servizi certificati" (Installazione di Servizi certificati a pagina 149).

Per accedere alle informazioni relative a un certificato, fare clic su **Administration>Security>SSL Certificate** (Amministrazione>Protezione>Certificato SSL). Nella scheda SSL Certificate (Certificato SSL) vengono visualizzate le seguenti informazioni:

- Nel campo Issued To (Emesso a) è indicata l'entità a favore della quale è stato emesso il certificato.
- Nel campo Issued By (Emesso da) è indicata l'autorità di certificazione che ha emesso il certificato.
- Nel campo Valid From (Valido da) è riportata la data di inizio validità del certificato.
- Nel campo Valid Until (Valido fino a) è riportata la data di scadenza del certificato.
- Nel campo Serial Number (Numero di serie) è indicato il numero di serie assegnato al certificato dall'autorità di certificazione.

Nella scheda SSL Certificate (Certificato SSL) sono disponibili le seguenti opzioni:

- Create Certificate Request (Crea richiesta di certificato) – Utilizzare questo pulsante per creare una richiesta di certificato. Quando si fa clic su questo pulsante, viene creata una richiesta di certificato (in formato PKCS #10) che è possibile inviare a un'autorità di certificazione. La richiesta di certificato è crittografata in Base64. L'autorità di certificazione elaborerà la richiesta e invierà la risposta (Certificato X.509) che potrà essere importata in iLO 2.

  La richiesta di certificato contiene una coppia di chiavi pubblica e privata che viene utilizzata per convalidare le comunicazioni tra il browser del client e iLO 2. La richiesta di certificato generata viene mantenuta in memoria finché non viene generata una nuova richiesta, non viene reimpostato iLO 2 o non viene importato un certificato dal processo di generazione. È possibile generare la richiesta di certificato e copiarla negli Appunti del client, disconnettersi dal sito Web di iLO 2 per il recupero del certificato, quindi ricollegarsi per importare il certificato.

  Quando si inoltra una richiesta all'autorità di certificazione, assicurarsi di eseguire le seguenti attività:

  a. Utilizzare il nome iLO 2 elencato nella schermata System Status (Stato sistema) come URL per il server.

  b. Richiedere che il certificato venga generato in formato RAW.

  c. Includere le righe del certificato `Begin` e `End`.

  Ogni volta che si fa clic su **Create Certificate Request** (Crea richiesta di certificato), viene generata una nuova richiesta di certificato anche se il nome iLO 2 è lo stesso.

- Import Certificate (Importa certificato) – Utilizzare questo pulsante quando si visualizza nuovamente la pagina Certificate Administration (Amministrazione certificato) per importare un certificato. Fare clic su **Import Certificate** (Importa certificato) per passare direttamente alla pagina Certificate Import (Importazione certificato) senza creare una nuova richiesta di certificato. Un certificato funziona solo con le chiavi generate per la richiesta di certificato originale a partire dalla

quale è stato creato. Se, dall'invio della richiesta di certificato originale a un'autorità di certificazione, iLO 2 è stato reimpostato o è stata generata un'altra richiesta di certificato, è necessario generare una nuova richiesta di certificato e inviarla all'autorità di certificazione.

È possibile creare una richiesta di certificato o importare un certificato esistente mediante i comandi XML di RIBCL. Questi comandi consentono di eseguire automaticamente la configurazione dei certificati tramite script sui server iLO 2 anziché configurare i certificati manualmente mediante l'interfaccia del browser. Per ulteriori informazioni, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

Autenticazione basata su due fattori

L'accesso a iLO 2 richiede l'autenticazione utente. Questa versione di firmware include uno schema di autenticazione avanzato per iLO 2 basato su due fattori di autenticazione, ovvero una password o un codice PIN e una chiave privata per un certificato digitale. Per eseguire l'autenticazione basata su due fattori è necessario verificare la propria identità specificando entrambi i fattori. È possibile memorizzare i certificati digitali e le chiavi private su qualsiasi supporto, ad esempio una smart card, un'unità USB o un'unità disco rigido.

La scheda Two-Factor Authentication (Autenticazione basata su due fattori) consente di configurare le impostazioni di protezione e di verificare, importare o eliminare un certificato CA attendibile. L'impostazione Two-Factor Authentication Enforcement (Abilitazione autenticazione basata su due fattori) consente di stabilire se tale funzione verrà utilizzata per l'autenticazione dell'utente durante l'accesso. Per richiedere l'autenticazione basata su due fattori, fare clic su **Enabled** (Abilitato). Per disattivare la richiesta di autenticazione basata su due fattori e per consentire all'utente di eseguire l'accesso utilizzando soltanto il nome utente e la password, fare clic su **Disabled** (Disabilitato). Se non è stato configurato un certificato CA attendibile, non è possibile assegnare all'impostazione il valore Enabled (Abilitato). Per fornire la necessaria protezione, vengono apportate le seguenti modifiche di configurazione quando l'autenticazione a due fattori è abilitata:

- Accesso Telnet: Disabilitato
- Secure Shell (SSH) Access (Accesso Secure Shell (SSH)): Disabilitato
- Serial Command Line Interface Status (Stato interfaccia riga di comando seriale): Disabilitato

Se è necessario un accesso Telnet, SSH o Serial CLI, abilitare di nuovo queste impostazioni dopo l'abilitazione basata su due fattori. Tuttavia, poiché questi metodi di accesso non supportano l'autenticazione basata su due fattori, per accedere a iLO 2 tramite Telnet, SSH o Serial CLI è necessario un solo fattore.

Se viene abilitata l'autenticazione basata su due fattori, l'accesso mediante l'utility CPQLOCFG verrà disabilitato, poiché quest'ultima non è in grado di soddisfare tutti i requisiti di autenticazione. L'utility HPONCFG rimarrà invece abilitata, poiché per la relativa esecuzione è necessario disporre di privilegi di amministratore nel sistema host.

Per il funzionamento dell'autenticazione basata su due fattori, è necessario un certificato CA attendibile. Se tale certificato non è configurato, non è possibile impostare Two-Factor Authentication Enforcement (Abilitazione autenticazione basata su due fattori) su Enabled (Abilitato). Inoltre, se si utilizzano account utente locali, è necessario associare un certificato client a un account utente locale. Se iLO 2 sta utilizzando l'autenticazione di directory, l'associazione del certificato del client agli account utente locali è opzionale.

Per modificare le impostazioni dell'autenticazione basata su due fattori per iLO 2:

1. Accedere a iLO 2 usando un account che dispone del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).
2. Fare clic su **Administration>Security>Two-Factor Authentication** (Amministrazione>Protezione>Autenticazione basata su due fattori).
3. Modificare le impostazioni immettendo i valori desiderati nei campi.
4. Fare clic su **Apply** (Applica) per salvare le modifiche.

L'impostazione Certificate Revocation Checking (Verifica revoca certificati) controlla se iLO 2 utilizza l'attributo relativo ai punti di distribuzione CRL per scaricare il CRL più recente e per verificare se il certificato del client è stato revocato. Se il certificato del client è contenuto nel CRL o se quest'ultimo non può essere scaricato per qualsiasi motivo, l'accesso viene negato. Se Certificate Revocation Checking (Verifica revoca certificati) è impostata su **Yes** (Sì), il punto di distribuzione CRL deve essere disponibile e accessibile per iLO 2.

L'impostazione Certificate Owner Field (Campo proprietario certificato) specifica quale attributo del certificato del client deve essere utilizzato quando si effettua l'autenticazione della directory. Utilizzare questa impostazione solo se l'autenticazione della directory è abilitata. Il valore di Certificate Owner Field (Campo proprietario certificato) dipende dalla versione del supporto di directory utilizzata, dalla configurazione della directory e dai criteri relativi al rilascio dei certificati utilizzati dall'organizzazione. Se è stato specificato SAN, iLO 2 estrae il nome principale utente dal nome alternativo oggetto e lo utilizza per l'autenticazione con la directory, ad esempio nomeutente@dominio.estensione. Ad esempio, se il nome del soggetto è `/DC=com/DC=domain/OU=organization/CN=user`, iLO 2 deriverà `CN=user,OU=organization,DC=domain,DC=com`.

Configurazione per il primo utilizzo dell'autenticazione basata su due fattori

Quando si configura l'autenticazione basata su due fattori per il primo utilizzo, è possibile utilizzare account utente locali o account utente di directory. Per ulteriori informazioni sulle impostazioni della funzione di autenticazione basata su due fattori, vedere la sezione "Autenticazione basata su due fattori" (Autenticazione basata su due fattori a pagina 44).

Impostazione degli account utente locali

1. Ottenere il certificato pubblico dell'autorità che emette certificati o smart card nell'organizzazione.
2. Esportare il certificato in formato crittografato in Base64 in un file sul desktop, ad esempio, CAcert.txt.
3. Ottenere il certificato pubblico dell'utente che necessita dell'accesso a iLO 2.
4. Esportare il certificato in formato crittografato in Base64 in un file sul desktop, ad esempio, Usercert.txt.
5. Aprire il file CAcert.txt nel Blocco note, selezionare tutto il testo e copiarlo premendo i tasti **Ctrl+C**.
6. Accedere a iLO 2 e visualizzare la pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori).
7. Fare clic su **Import Trusted CA Certificate** (Importa certificato CA attendibile). Viene visualizzata la pagina Import Root CA Certificate (Importa certificato attendibile principale).
8. Fare clic sull'area di testo bianca in modo da posizionare il cursore all'interno di tale area, quindi incollare il contenuto degli Appunti premendo la combinazione di tasti **Ctrl+V**.

9. Fare clic su **Import Root CA Certificate** (Importa certificato CA principale). Viene visualizzata di nuovo la pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori) con alcune informazioni visualizzate in Trusted CA Certificate Information (Informazioni certificato CA attendibile).
10. Dal desktop, aprire il file del certificato dell'utente nel Blocco note, selezionare tutto il testo e copiarlo premendo la combinazione di tasti **Ctrl+C**.
11. Sfogliare fino alla pagina User Administration (Amministrazione utenti) in iLO 2 e selezionare l'utente per il quale si è ottenuto un certificato pubblico oppure creare un nuovo utente.
12. Fare clic su **View/Modify** (Visualizza/Modifica).
13. Fare clic su **Add a certificate** (Aggiungi certificato).
14. Fare clic sull'area di testo bianca in modo da posizionare il cursore all'interno di tale area, quindi incollare il contenuto degli Appunti premendo la combinazione di tasti **CTRL+V**.
15. Fare clic su **Add user Certificate** (Aggiungi certificato utente). Verrà visualizzata di nuovo la pagina Modify User (Modifica utente), con un numero a 40 cifre nel campo Thumbprint (Identificazione personale). È possibile utilizzare Microsoft® Certificate Viewer per confrontare il numero con le informazioni di identificazione personale visualizzate per il certificato.
16. Accedere alla pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori).
17. Impostare l'opzione Two-Factor Authentication (Autenticazione basata su due fattori) su **Enabled** (Abilitato).
18. Impostare l'opzione Certificate Revocation Checking (Verifica revoca certificato) su **Disabled** (Disabilitato). Questa opzione rappresenta il valore predefinito.
19. Fare clic su **Apply** (Applica). iLO 2 viene reimpostato. Quando iLO 2 tenterà di passare di nuovo alla pagina di accesso, nel browser verrà visualizzata la pagina Client Authentication (Autenticazione client) con l'elenco di certificati disponibili per il sistema.

    Se il certificato utente non è registrato nel computer client, non verrà visualizzato nell'elenco. È necessario registrare il certificato utente nel sistema client prima di utilizzarlo. Se nel sistema client non esiste alcun certificato client, non verrà visualizzata la pagina Client Authentication (Autenticazione client) ma l'errore Page cannot be displayed (Impossibile visualizzare la pagina). Per risolvere l'errore, è necessario registrare il certificato client nel computer client. Per ulteriori informazioni sull'esportazione e la registrazione di certificati client, consultare la documentazione fornita con la smart card oppure contattare l'autorità di certificazione.
20. Selezionare il certificato aggiunto all'utente in iLO 2. Fare clic su **OK**.
21. Se richiesto, inserire la smart card oppure immettere il PIN o la password.

Una volta completato il processo di autenticazione, è possibile accedere a iLO 2.

Impostazione degli account utente di directory

1. Ottenere il certificato pubblico dell'autorità che emette certificati o smart card nell'organizzazione.
2. Esportare il certificato in formato crittografato in Base64 in un file sul desktop, ad esempio, CAcert.txt.
3. Aprire il file nel Blocco note, selezionare tutto il testo e copiare il contenuto negli Appunti premendo la combinazione di tasti **Ctrl+C**.
4. Accedere a iLO 2 e visualizzare la pagina **Two-Factor Authentication Settings** (Impostazioni autenticazione basata su due fattori).

5. Fare clic su **Import Trusted CA Certificate** (Importa certificato CA attendibile). Viene visualizzata un'altra pagina.
6. Fare clic sull'area di testo bianca in modo da posizionare il cursore all'interno di tale area, quindi incollare il contenuto degli Appunti premendo la combinazione di tasti **Ctrl+V**.
7. Fare clic su **Import Root CA Certificate** (Importa certificato CA principale). Viene visualizzata di nuovo la pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori) con alcune informazioni visualizzate in Trusted CA Certificate Information (Informazioni certificato CA attendibile).
8. Modificare l'impostazione di Enforce Two-Factor Authentication (Abilita autenticazione a due fattori) su **Yes** (Sì).
9. Impostazione Certificate Revocation Checking (Verifica revoca certificato) su **No (default)** (No (predefinito)).
10. Modificare l'impostazione Certificate Owner Field (Campo proprietario certificato) su **SAN**. Per ulteriori informazioni, vedere la sezione "Autenticazione basata su due fattori" (Autenticazione basata su due fattori a pagina 44).
11. Fare clic su **Apply** (Applica). iLO 2 viene reimpostato. Quando iLO 2 tenterà di passare di nuovo alla pagina di accesso, nel browser verrà visualizzata la pagina Client Authentication (Autenticazione client) con l'elenco di certificati disponibili per il sistema.
12. Selezionare il certificato aggiunto all'utente in iLO 2. Fare clic su **OK**.
13. Se richiesto, inserire la smart card oppure immettere il PIN o la password. Verrà visualizzata la pagina di accesso con l'indirizzo di posta elettronica dell'utente nel campo Directory User (Utente di directory). Non è possibile modificare le informazioni contenute nel campo Directory User (Utente di directory).
14. Immettere la password dell'utente di directory. Fare clic su **Login** (Accesso).

Una volta completato il processo di autenticazione, è possibile accedere a iLO 2. Per ulteriori informazioni sulla configurazione degli utenti di directory e dei relativi privilegi, vedere la sezione "Impostazioni di directory" (Impostazioni di directory a pagina 50).

Impostazione di un utente per l'autenticazione basata su due fattori

Per autenticare un utente con account locale iLO 2, è necessario associare un certificato al nome utente locale. Se è stato associato un certificato all'utente, nella pagina Administration>Modify User (Amministrazione>Modifica utente) vengono visualizzate informazioni di identificazione personale (hash SHA1 del certificato) e un pulsante che rimuove il certificato. Se, invece, non è stato associato alcun certificato all'utente, viene visualizzato il messaggio `Thumbprint: A certificate has NOT been mapped to this user` (Identificazione personale: NON è presente alcun certificato associato a questo utente) e un pulsante che consente di avviare il processo di importazione del certificato.

Per impostare un utente per l'autenticazione basata su due fattori e aggiungere un certificato utente:

1. Accedere a iLO 2 usando un account che dispone del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).
2. Fare clic su **Administration>User Administration** (Amministrazione>Amministrazione utenti). Selezionare un utente.
3. Fare clic su **View/Modify** (Visualizza/Modifica).

4. Nella sezione User Certificate Information (Informazioni certificato utente), fare clic su **Add a certificate** (Aggiungi certificato).
5. Nella pagina Map User Certificate (Associa certificato utente), incollare il certificato utente nella casella di testo e fare clic su **Import Certificate** (Importa certificato). Per ulteriori informazioni sulla creazione, la copia e l'inserimento delle informazioni del certificato, vedere la sezione "Configurazione per il primo utilizzo dell'autenticazione basata su due fattori" (Configurazione per il primo utilizzo dell'autenticazione basata su due fattori a pagina 45).

Accesso tramite autenticazione basata su due fattori

Quando si accede a iLO 2 ed è necessario eseguire l'autenticazione basata su due fattori, viene visualizzata la pagina Client Authentication (Autenticazione client) con la richiesta di selezionare il certificato che si desidera utilizzare. Nella pagina Client Authentication (Autenticazione client) sono visualizzati tutti i certificati disponibili per autenticare un client. Selezionare il certificato appropriato. Il certificato può essere costituito da un certificato associato a un utente locale in iLO 2 o da un certificato specifico dell'utente emesso per eseguire l'autenticazione nel dominio.

Dopo avere selezionato un certificato, se quest'ultimo è protetto con una password o se è memorizzato in una smart card, verrà visualizzata una seconda pagina che richiederà di immettere il PIN o la password associati al certificato selezionato.

La firma del certificato viene confrontata con quella configurata in iLO 2 per verificare che sia stato emesso da un'autorità di certificazione attendibile. iLO 2 controlla inoltre se il certificato è stato revocato e se è associato a un utente nel database degli utenti locali di iLO 2. Se tutte le verifiche hanno esito positivo, verrà visualizzata la normale interfaccia utente di iLO 2.

Se, al contrario, la procedura di autenticazione delle credenziali ha esito negativo, viene visualizzata la pagina Login Failed (Accesso non riuscito). In questo caso, verrà richiesto di chiudere il browser, aprire una nuova pagina del browser e collegarsi di nuovo. Se l'autenticazione dell'utente locale ha esito negativo ed è abilitata l'autenticazione di directory, RILOE II visualizza una pagina di accesso con il campo Directory user (Utente directory) compilato con il nome principale utente, ricavato dal certificato, o con il nome distinto, derivato dal soggetto del certificato. Per questo account utente, è necessaria una password. Dopo aver inserito la password, la procedura di autenticazione è completata.

Utilizzo dell'autenticazione basata su due fattori con autenticazione di directory

In alcuni casi, la configurazione dell'autenticazione basata su due fattori con autenticazione di directory risulta alquanto complicata. In iLO 2 è possibile utilizzare lo schema esteso o lo schema di directory predefinito HP per effettuare l'integrazione con i servizi di directory. Se l'autenticazione basata su due fattori è abilitata, per assicurare la protezione iLO 2 utilizza un attributo del certificato client come nome di accesso dell'utente di directory. L'impostazione di configurazione Certificate Owner Field (Campo proprietario certificato) disponibile nella pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori) stabilirà quale attributo del certificato client verrà utilizzato da iLO 2. Se Certificate Owner Field (Campo proprietario certificato) è impostato su SAN, iLO 2 ottiene il nome di accesso dell'utente di directory dall'attributo UPN di SAN. Se Certificate Owner Field (Campo proprietario certificato) è impostato su Subject (Soggetto), iLO 2 ottiene il nome distinto dell'utente di directory dal soggetto del certificato.

La scelta dell'impostazione di Certificate Owner Field (Campo proprietario certificato) dipende dal metodo di integrazione delle directory utilizzato, dal tipo di progettazione dell'architettura di queste ultime e dalle informazioni contenute nei certificati utente rilasciati. Gli esempi seguenti presuppongono che si disponga delle autorizzazioni necessarie.

Autenticazione tramite lo schema di directory predefinito, parte 1: Il nome distinto di un utente di directory è CN=John Doe, OU=IT, DC=MyCompany, DC=com. Di seguito sono riportati gli attributi del certificato di John Doe:

- Oggetto: DC=com/DC=MyCompany/OU=IT/CN=John Doe
- SAN/UPN: john.doe@MyCompany.com

L'autenticazione in iLO 2 mediante il nome utente john.doe@MyCompany.com e una password funzionerà se l'autenticazione basata su due fattori **non** è stata abilitata. Una volta abilitata l'autenticazione basata su due fattori, se viene selezionata l'impostazione SAN nella pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori), nel campo Directory User (Utente directory) della pagina di accesso verrà automaticamente immesso john.doe@MyCompany.com. È possibile immettere la password, ma l'utente **non** verrà autenticato. L'utente non è autenticato perché john.doe@MyCompany.com, il nome distinto ottenuto dal certificato, non è il nome distinto dell'utente di directory. In questo caso, è necessario selezionare **Subject** (Soggetto) nella pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori). A questo punto, il campo Directory User (Utente directory) nella pagina di accesso verrà popolato con CN=John Doe, OU=IT DC=MyCompany e DC=com, ovvero il nome distinto attuale dell'utente. Se viene immessa la password corretta, l'utente verrà autenticato.

Autenticazione tramite lo schema di directory predefinito, parte 2: Il nome distinto di un utente di directory è CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com. Di seguito sono riportati gli attributi del certificato di John Doe:

- Oggetto: DC=com/DC=MyCompany/OU=Employees/CN=John Doe/ E=john.doe@MyCompany.com
- SAN/UPN: john.doe@MyCompany.com
- Nella pagina Directory Settings (Impostazioni di directory), il contesto di ricerca è impostato su: OU=IT, DC=MyCompany, DC=com

In questo esempio, se SAN viene selezionato nella pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori), nel campo Directory User (Utente directory) disponibile nella pagina di accesso viene inserito john.doe@MyCompany.com. Dopo l'immissione della password corretta, l'utente verrà autenticato. L'utente verrà autenticato anche se john.doe@MyCompany.com non è il suo nome distinto. L'utente viene autenticato perché iLO 2 tenta di farlo utilizzando i campi del contesto di ricerca (CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com) configurati nella pagina Directory Settings (Impostazioni di directory). Poiché si tratta del nome distinto corretto, iLO 2 trova con successo l'utente nella directory.

NOTA: Selezionare l'impostazione Subject (Soggetto) nella pagina Two-Factor Authentication Settings (Impostazioni autenticazione basata su due fattori), poiché il soggetto del certificato non è il nome distinto dell'utente nella directory.

Se si esegue l'autenticazione utilizzando lo schema esteso HP, HP raccomanda di selezionare l'opzione SAN nella pagina Two-factor Authentication Settings (Impostazioni autenticazione basata su due fattori).

Impostazioni di directory

Per le procedure di autorizzazione e autenticazione degli utenti, è possibile collegare iLO 2 a Microsoft® Active Directory, Novell e-Directory o ad altri servizi di directory conformi allo standard LDAP 3.0. Ad esempio, è possibile configurare iLO 2 in modo da eseguire l'autenticazione e l'autorizzazione degli utenti ricorrendo all'integrazione di directory tramite schema HP o senza schema. Per il collegamento ai servizi di directory, iLO 2 utilizza esclusivamente connessioni protette da SSL alla porta LDAP del server di directory. Per impostazione predefinita, il numero della porta LDAP protetta è 636. Per usufruire del supporto dei servizi di directory, è necessario acquistare una licenza aggiuntiva opzionale. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20). Per informazioni più dettagliate sulle directory, vedere la sezione "Servizi di directory" (Servizi di directory a pagina 145).

Gli account utente memorizzati localmente, disponibili nella pagina User Administration (Amministrazione utenti), possono rimanere attivi anche quando è abilitata la funzione di supporto delle directory di iLO 2. In questo modo, è consentito sia l'accesso basato su directory che l'accesso da computer locale. In genere, inoltre, un amministratore può eliminare account utente locali (ad eccezione degli account di accesso di emergenza) dopo la configurazione di iLO 2 per l'accesso ai servizi di directory. Se è abilitata la funzione di supporto delle directory, è possibile disattivare l'accesso a questi account.

Configurazione delle impostazioni di directory

iLO 2 consente agli amministratori di gestire gli account utente da una posizione centralizzata utilizzando i servizi di directory. Per configurare e verificare i servizi di directory di iLO 2, è necessario disporre del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2). Per accedere alla scheda Directory Settings (Impostazioni di directory), fare clic su **Administration>Security>Directory** (Amministrazione>Protezione>Directory).

Le impostazioni relative alla directory di iLO 2 consentono di controllare il comportamento correlato alla directory di iLO 2 a cui si è connessi. Sono incluse le seguenti impostazioni:

- Disable Directory Authentication (Disabilita autenticazione directory) – Consente di attivare o disattivare il supporto per directory sulla directory di iLO 2.
  - Se l'autenticazione tramite directory è abilitata e configurata correttamente, gli utenti possono accedere tramite le credenziali di directory.
  - Se l'autenticazione tramite directory è disabilitata, le credenziali utente non vengono convalidate tramite la directory.
- Use HP Extended Schema (Utilizza schema esteso HP) – Consente di selezionare l'autenticazione e l'autorizzazione tramite directory utilizzando gli oggetti di directory creati con lo schema HP. Selezionare questa opzione se la directory è stata estesa con lo schema HP e si prevede di utilizzarla.
- Use Directory Default Schema (Utilizza schema di directory predefinito) – Consente di selezionare l'autenticazione e l'autorizzazione tramite directory utilizzando gli account utente nella directory. Selezionare questa opzione se la directory non è stata estesa con lo schema HP. Per l'autenticazione e l'autorizzazione degli utenti vengono utilizzati gli account utente e le appartenenze ai gruppi. Dopo aver specificato le informazioni di rete della directory, fare clic su **Administer Groups** (Amministra gruppi) e immettere uno o più nomi distinti di directory validi e i privilegi per concedere agli utenti l'accesso a iLO 2.
- Local User Accounts (Account utente locali) – Consente di limitare l'accesso agli utenti locali.
  - Se questa opzione è abilitata, un utente può accedere utilizzando le credenziali utente memorizzate in locale.
  - Se invece è disabilitata, l'accesso degli utenti è limitato alle credenziali di directory valide.

    L'accesso tramite account utente locali è abilitato se il supporto per directory è disabilitato e/o la licenza iLO 2 Select o iLO 2 Advanced è stata revocata. Non è possibile disabilitare questo tipo di accesso se è stata effettuata la connessione tramite un account utente locale.

Le impostazioni relative al server di directory di iLO 2 consentono di identificare l'indirizzo e la porta di tale server. Sono incluse le seguenti impostazioni:

- Directory Server Address (Indirizzo server di directory) – Consente di specificare il nome DNS di rete o l'indirizzo IP del server di directory. È possibile specificare più server, separati da una virgola (,) o da uno spazio ( ). Se l'opzione Use Directory Default Schema (Utilizza schema di directory predefinito) è selezionata, immettere un nome DNS nel campo Directory Server Address (Indirizzo server di directory) per consentire l'autenticazione con l'ID utente. Ad esempio:

```
directory.hp.com
192.168.1.250, 192.168.1.251
```

- Directory Server LDAP Port (Porta LDAP server di directory) – Consente di specificare il numero di porta per il servizio LDAP protetto sul server. Il valore predefinito per questa porta è 636. È tuttavia possibile specificare un altro valore se il servizio di directory è configurato per l'uso di una porta differente.
- iLO 2 Directory Properties (Proprietà directory iLO 2) – Identifica l'oggetto LOM nella struttura di directory. Queste informazioni vengono utilizzate per determinare i diritti di accesso degli utenti. È possibile configurare iLO 2 con la password per l'oggetto LOM in questo momento, anche se queste informazioni non vengono utilizzate finché non viene fornito il supporto per la configurazione della directory.
- LOM Object Distinguished Name (Nome distinto oggetto LOM) – Specifica la posizione dell'istanza LOM nella struttura di directory. Ad esempio: cn=iLO 2 Mail Server,ou=Management Devices,o=hp

  I contesti di ricerca utente non vengono applicati al nome distinto dell'oggetto LOM quando si accede al server di directory.
- LOM Object Password (Password oggetto LOM) – Specifica la password relativa all'oggetto utilizzato da iLO 2 per verificare se sono presenti aggiornamenti nella directory (LOM Object Distinguished Name).
- Confirm Password (Conferma password) – Consente di confermare la password dell'oggetto LOM. Se si modifica il valore di LOM Object Password (Password oggetto LOM), reimmettere la nuova password in questo campo.
- I contesti di ricerca per l'accesso utente consentono di specificare i sottocontesti di directory comuni per evitare agli utenti di immettere il nome distinto completo al momento dell'accesso.

  È possibile identificare tutti gli oggetti elencati in una directory utilizzando i relativi nomi distinti univoci. Tuttavia, i nomi distinti possono avere una lunghezza notevole ed è possibile che gli utenti non conoscano i rispettivi nomi distinti o dispongano di account in contesti di directory differenti. iLO 2 tenta di contattare il servizio di directory in base al nome distinto, quindi applica i contesti di ricerca nell'ordine specificato finché l'accesso non riesce.

  I contesti utente di directory specificano i contesti di ricerca che vengono applicati al nome di accesso.

  Esempio 1:

  Anziché eseguire l'accesso come cn=user,ou=engineering,o=hp è possibile utilizzare il contesto di ricerca `ou=engineering,o=hp` per accedere come `user`

  Esempio 2:

  Se un sistema viene gestito da Information Management, Services e Training, i seguenti contesti di ricerca:

```
Directory User Context 1:ou=IM,o=hp
Directory User Context 2:ou=Services,o=hp
Directory User Context 3:ou=Training,o=hp
```

consentono agli utenti presenti in una qualsiasi di queste organizzazioni di accedere utilizzando i rispettivi nomi comuni. Se un utente è presente sia nell'unità organizzativa IM che in Training, l'accesso viene prima tentato come cn=user,ou=IM,o=hp.

Esempio 3 (solo Active Directory):

Microsoft Active Directory consente un formato di credenziali utente alternativo. I contesti di ricerca in questo formato possono essere verificati solo mediante un tentativo di accesso. Un utente può eseguire l'accesso come:

```
user@domain.hp.com
in which case a search context of
@domain.hp.com
allows the user to login as
user
```

Per verificare la comunicazione tra il server di directory e iLO 2, fare clic su **Test Settings** (Verifica impostazioni). Per ulteriori informazioni, vedere la sezione "Verifiche di directory" (Verifiche di directory a pagina 53).

Verifiche di directory

Per convalidare le impostazioni di directory correnti di iLO 2, fare clic sul pulsante **Test Settings** (Verifica impostazioni) nella pagina Directory Settings (Impostazioni di directory). Viene visualizzata la pagina delle verifiche di directory.

Questa pagina visualizza i risultati di una serie di semplici test utilizzati per convalidare le impostazioni delle directory correnti. Essa include inoltre un registro di test che visualizza i risultati e gli eventuali problemi rilevati. Se le impostazioni di directory sono state configurate correttamente, non è necessario eseguire nuovamente questi test. La schermata Directory Tests (Verifiche di directory) non richiede l'accesso come utente di directory.

Per verificare le impostazioni della directory:

1. Immettere il nome distinto e la password di un amministratore di directory. È consigliabile immettere le stesse credenziali utilizzate per la creazione degli oggetti di iLO 2 nella directory. Queste credenziali non vengono memorizzate da iLO 2. Sono utilizzate per verificare i contesti di ricerca degli utenti e degli oggetti di iLO 2.
2. Immettere anche un nome utente e una password di verifica. Normalmente si tratta di un account utilizzato per l'accesso a iLO 2 sul quale viene eseguito il test. Questo account può essere uguale a quello dell'amministratore della directory. Tuttavia, i test non possono verificare l'autenticazione dell'utente con un account "superutente". Queste credenziali non vengono memorizzate da iLO 2.
3. Fare clic su **Start Test** (Avvia test). Una serie di test in background vengono avviati, a cominciare da un ping di rete dell'utente della directory alla connessione SSL sul server, e i privilegi dell'utente come durante un normale accesso vengono valutati.

Durante l'esecuzione dei test, la pagina viene periodicamente aggiornata. L'utente può interrompere i test in qualsiasi momento o aggiornare manualmente la pagina. Per informazioni dettagliate sui test e sulle operazioni da eseguire in caso di problemi, fare clic sul collegamento alla Guida in linea della pagina.

Crittografia

iLO 2 fornisce funzionalità di protezione avanzate per la gestione remota in ambienti IT distribuiti, proteggendo i dati del browser Web tramite crittografia SSL. La crittografia SSL dei dati HTTP garantisce la protezione dei dati durante la trasmissione attraverso la rete. iLO 2 fornisce il supporto per due delle più potenti codifiche disponibili: AES (Advanced Encryption Standard) e 3DES (Triple Data Encryption Standard). In iLO 2 sono supportate le seguenti codifiche:

- AES a 256 bit con RSA, DHE e SHA1 MAC
- AES a 256 bit con RSA e SHA1 MAC
- AES a 128 bit con RSA, DHE e SHA1 MAC
- AES a 128 bit con RSA e SHA1 MAC
- Triple DES a 168 bit con RSA e SHA1 MAC
- Triple DES a 168 bit con RSA, DHE e SHA1 MAC

iLO 2 fornisce inoltre funzionalità di crittografia avanzate tramite la porta SSH per transazioni CLP protette. Tramite questa porta sono supportate le codifiche AES128-CBC e 3DES-CBC.

Se la crittografia AES/3DES è abilitata, iLO 2 impone l'uso di queste codifiche avanzate attraverso i canali protetti, ad esempio le trasmissioni HTTP protette tramite browser, porta SSH e porta XML. In questo caso, per connettersi a iLO 2 tramite questi canali è necessario utilizzare una codifica uguale o superiore a AES/3DES. Le comunicazioni e le connessioni tramite canali meno protetti (ad esempio la porta Telnet) non sono interessate dall'impostazione della crittografia AES/3DES.

Per impostazione predefinita, per i dati della console remota viene utilizzata la crittografia bidirezionale RC4 a 128 bit. L'utility CPQLOCFG utilizza una codifica Triple DES a 168 bit con RSA e SHA1 MAC per inviare in modo protetto gli script RIBCL a iLO 2 attraverso la rete.

Impostazioni di crittografia

È possibile visualizzare o modificare le impostazioni di crittografia correnti utilizzando l'interfaccia di iLO 2, CLP o RIBCL.

Per visualizzare o modificare le impostazioni di crittografia correnti tramite l'interfaccia di iLO 2:

1. Fare clic su **Administration>Security>Encryption** (Amministrazione>Protezione>Crittografia).

   Viene visualizzata la pagina Encryption (Crittografia), in cui sono definite le impostazioni di crittografia correnti per iLO 2, ossia la codifica negoziata corrente e le impostazioni di abilitazione della crittografia.

   - Current Negotiated Cipher (Codifica negoziata corrente) visualizza la codifica in uso per la sessione del browser corrente. Dopo l'esecuzione dell'accesso a iLO 2 tramite browser, il browser e iLO 2 negoziano un'impostazione di codifica da utilizzare durante la sessione. Nella sezione Current Negotiated Cipher (Codifica negoziata corrente) della pagina Encryption (Crittografia) viene visualizzata la codifica negoziata.

     Encryption Enforcement Settings (Impostazioni abilitazione crittografia) visualizza le impostazioni di crittografia correnti per iLO 2. L'opzione Enforce AES/3DES Encryption (Imponi crittografia AES/3DES), se abilitata, consente a iLO 2 di accettare solo connessioni tramite browser e interfaccia SSH in grado di soddisfare il livello minimo di codifica. Se questa opzione è abilitata, per la connessione a iLO 2 è necessario utilizzare almeno il livello di codifica AES o 3DES. Enforce AES/3DES Encryption (Imponi crittografia AES/3DES) può essere abilitata o disabilitata.

2. Per salvare le modifiche, fare clic su **Apply** (Applica).

Quando si abilita l'opzione di imposizione della crittografia, dopo aver fatto clic su **Apply** (Applica) chiudere tutti i browser aperti. Gli eventuali browser rimasti aperti potrebbero continuare a utilizzare una codifica diversa da AES/3DES.

Per visualizzare o modificare le impostazioni di crittografia correnti tramite CLP o RIBCL, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

Connessione a iLO 2 con crittografia AES/3DES

Quando è abilitata l'opzione Enforce AES/3DES Encryption (Imponi crittografia AES/3DES), iLO 2 richiede la connessione tramite canali protetti (browser Web, porta SSH o porta XML) con almeno un livello di codifica AES o 3DES.

Per la connessione a iLO 2 tramite browser, è necessario configurare il browser con almeno un livello di codifica AES o 3DES. Se il browser Web non utilizza codifiche AES o 3DES, iLO 2 visualizza un messaggio di errore per segnalare all'utente che è necessario chiudere la connessione corrente e selezionare la codifica corretta.

Per selezionare almeno un livello di codifica AES o 3DES, consultare la documentazione del browser. I browser utilizzano metodi differenti per la selezione di una codifica negoziata. Prima di cambiare il livello di codifica del browser, è necessario disconnettersi da iLO 2 tramite il browser corrente. Se si apportano modifiche all'impostazione relativa alla codifica del browser senza disconnettersi da iLO 2, è possibile che il browser continui a utilizzare una codifica diversa da AES/3DES.

Tutti i sistemi operativi client e i browser supportati da iLO 2 sono in grado di supportare la funzionalità di crittografia AES/3DES di iLO 2, fatta eccezione per Windows 2000 Professional con Internet Explorer. Per impostazione predefinita, Windows 2000 Professional non supporta codifiche AES o 3DES. Se nel client è installato Windows® 2000 Professional, è necessario utilizzare un altro browser o aggiornare il sistema operativo.

Internet Explorer non presenta un'impostazione di livello di codifica selezionabile dall'utente. È necessario modificare il registro di sistema per consentire a Internet Explorer di connettersi a iLO 2 quando l'opzione Enforce AES/3DES Encryption (Imponi crittografia AES/3DES) è abilitata. Per abilitare la crittografia AES/3DES in Internet Explorer, aprire il registro di sistema e impostare `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy` su 1.

NOTA: La modifica errata del registro può danneggiare seriamente il sistema. HP raccomanda di creare una copia di backup dei dati importanti sul computer prima di apportare modifiche al registro. Per informazioni sul ripristino del Registro di sistema, consultare l'articolo della Knowledge Base Microsoft (http://support.microsoft.com/kb/307545).

Per connettersi a iLO 2 tramite SSH, consultare la documentazione dell'utility SSH per informazioni sull'impostazione del livello di codifica.

Quando si esegue la connessione tramite il canale XML, per impostazione predefinita l'utility CPQLOCFG utilizza una codifica 3DES. CPQLOCFG 2.26 o versione successiva visualizza il seguente livello di codifica della connessione corrente nell'output XML. Ad esempio:

```
Connecting to Server..
Negotiated cipher: 168-bit Triple DES with RSA and a SHA1 MAC
```

La crittografia AES non è supportata da Internet Explorer sui client Windows® 2000 Professional. Per applicare la crittografia AES con questo sistema operativo, è necessario utilizzare un altro browser, ad esempio Mozilla.

HP SIM SSO

HP SIM SSO (Single sign-on, Accesso unificato) consente di passare direttamente da HP SIM al processore LOM, ignorando una fase di accesso intermedia. Per utilizzare SSO, è necessario disporre di una versione corrente di HP SIM e configurare il processore LOM in modo da accettare i collegamenti da HP SIM. Per il corretto funzionamento di HP SIM è necessario che siano stati installati gli aggiornamenti e le patch più recenti. Per ulteriori informazioni su HP Systems Insight Manager e sugli aggiornamenti disponibili, visitare il sito Web HP all'indirizzo http://www.hp.com/go/hpsim.

Per la funzionalità HP SIM SSO è necessario l'acquisto di licenze opzionali. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20).

La pagina HP SIM SSO consente di visualizzare e configurare le impostazioni di SSO tramite l'interfaccia di iLO 2. Per ulteriori informazioni, vedere la sezione "Impostazione di HP SIM SSO" (Impostazione di HP SIM SSO a pagina 58).

È inoltre possibile accedere alle impostazioni di configurazione di HP SIM SSO tramite script, file di testo e una riga di comando utilizzando client basati su testo, ad esempio SSH, attraverso la rete oppure direttamente dal sistema operativo sul computer host. La creazione di script SSO consente di utilizzare le stesse impostazioni SSO su tutti i processori LOM. Per ulteriori informazioni, script di esempio ed estensioni CLP per la lettura, la modifica e la scrittura delle impostazioni di configurazione di HP SIM SSO, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

Impostazione di iLO 2 per HP SIM SSO

Prima di iniziare l'impostazione di SSO, è necessario disporre dell'indirizzo di rete di HP SIM e assicurarsi che sia installata una chiave di licenza. Per impostare SSO:

1. Abilitare la modalità di attendibilità di Single Sign-On selezionando **Trust by Certificate** (Considera attendibile per certificato) (opzione consigliata), **Trust by Name** (Considera attendibile per nome) oppure **Trust All** (Considera attendibile tutti).
2. Aggiungere il certificato HP SIM del server a iLO 2.
   a. Fare clic su **Add an HP SIM Server** (Aggiungi server HP SIM).
   b. Immettere l'indirizzo di rete del server HP SIM.
   c. Fare clic su **Import Certificate** (Importa certificato).

      L'archivio dei certificati viene ridimensionato per consentire l'emissione di cinque certificati tipici di iLO 2. Tuttavia, se i certificati emessi non sono tipici, le relative dimensioni possono variare. Per i certificati e i nomi server di iLO 2 è allocato uno spazio di memorizzazione combinato pari a 6 KB. Una volta esaurito tale spazio, non vengono accettate altre importazioni.

Dopo l'impostazione di SSO in iLO 2, accedere a HP SIM, individuare il processore LOM e selezionare **Tools>System Information>iLO as...** (Strumenti>Informazioni di sistema>iLO come). HP SIM avvia un nuovo browser che si connette al processore di gestione LOM.

Aggiunta di server attendibili HP SIM

È possibile installare certificati server HP SIM utilizzando script adatti alla distribuzione di massa. Per ulteriori informazioni, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del*

processore di gestione HP Integrated Lights-Out. Per aggiungere record di server HP SIM tramite un browser:

1. Fare clic su **Administration>Security>HP SIM SSO** (Amministrazione>Protezione>HP SIM SSO).
2. Fare clic su **Add an HP SIM Server** (Aggiungi server HP SIM).
3. Per eseguire l'autenticazione del server, scegliere uno dei seguenti metodi:
   - Per aggiungere un server HP SIM utilizzando l'autenticazione Trust by Name (Considera attendibile per nome), immettere il nome di rete completo del server HP SIM nella sezione Add a Trusted HP SIM Server Name (Aggiungi nome server HP SIM attendibile). Fare clic su **Add Server Name** (Aggiungi nome server).

     L'autenticazione Trust by Name (Considera attendibile per nome) è basata su un nome di dominio completo, ad esempio sim-host.hp.com anziché sim-host. Se non si è sicuri riguardo al nome di dominio completo, utilizzare il comando `nslookup host`.
   - Per recuperare e importare un certificato da un server HP SIM attendibile, immettere il nome di rete completo di un server HP SIM nella sezione Retrieve and import a certificate from a trusted HP SIM Server (Recupera e importa certificato da server HP SIM attendibile). Fare clic su **Import Certificate** (Importa certificato) per richiedere il certificato al server HP SIM e importarlo automaticamente. Questo record supporta le autenticazioni di SSO Trust by Name (Considera attendibile per nome) e Trust by Certificate (Considera attendibile per certificato).

     Per impedire la manomissione di certificati, può essere opportuno importare direttamente un certificato server HP SIM. A questo scopo, recuperare la data del certificato HP SIM utilizzando una delle seguenti opzioni:
     - Utilizzando una finestra del browser separata, accedere al server HP SIM utilizzando il seguente URL:

       ```
       http://<sim network address>:280/GetCertificate
       ```

       Tagliare i dati del certificato da HP SIM e incollarli in iLO 2.
     - Esportare il certificato server HP SIM dall'interfaccia utente HP SIM selezionando **Options>Security>Certificates>Server Certificate** (Opzioni>Protezione>Certificati>Certificato server). Aprire il file mediante un editor di testo, copiare tutti i dati delle righe del certificato e incollarli in iLO 2.
     - Mediante gli strumenti della riga di comando sul server HP SIM, è possibile estrarre il certificato HP SIM utilizzando l'alias con codifica Tomcat per il certificato HP SIM. Ad esempio:

       ```
       mxcert -l tomcat
       ```

       I dati del certificato hanno il seguente aspetto:

       ```
       -----BEGIN CERTIFICATE-----
       several lines of encoded data
       -----END CERTIFICATE-----
       ```

     Dopo aver incollato i dati del certificato x.509 con codifica base-64 del server HP SIM nella sezione Directly import a HP SIM Server Certificate (Importa direttamente un certificato server HP SIM), fare clic su **Import Certificate** (Importa certificato) per registrare i dati. Questo tipo di record supporta le autenticazioni di SSO Trust by Name (Considera attendibile per nome) e Trust by Certificate (Considera attendibile per certificato).

Esistono altri metodi per recuperare i dati di un certificato server HP SIM. Per ulteriori informazioni, consultare la documentazione correlata.

Impostazione di HP SIM SSO

La pagina HP SIM SSO consente di visualizzare e configurare le impostazioni di Single Sign-On per iLO 2. Per modificare queste impostazioni, è necessario disporre del privilegio Configure iLO (Configura iLO). Per accedere alle impostazioni di SSO per iLO 2, fare clic su **Administration>Security>HP SIM SSO** (Amministrazione>Protezione>HP SIM SSO).

Nella pagina HP Systems Insight Manager Single Sign-On Settings (Impostazioni Single Sign-On di HP Systems Insight Manager) sono disponibili i seguenti campi e opzioni:

- Single Sign-On Trust Mode (Modalità attendibilità Single Sign-On) – Consente di controllare il modo in cui vengono accettate le connessioni avviate da SSO:
  - Trust None (Nessuna attendibilità) (impostazione predefinita) – Rifiuta tutte le richieste di connessione di SSO.
  - Trust by Certificate (Considera attendibile per certificato) (impostazione più sicura) – Consente le connessioni SSO solo da un server HP SIM con un certificato precedentemente importato in iLO 2.
  - Trust by Certificate (Considera attendibile per nome) – Consente le connessioni SSO da un server HP SIM con un nome DNS o certificato precedentemente importato in iLO 2.
  - Trust All (Considera attendibili tutti) (impostazione meno sicura) – Accetta le connessioni SSO avviate da un server HP SIM.

    Gli utenti che accedono a HP SIM sono autorizzati in base all'assegnazione dei ruoli sul server HP SIM. L'assegnazione dei ruoli viene passata al processore LOM durante il tentativo di esecuzione di SSO. È possibile configurare i privilegi di iLO 2 per ciascun ruolo nella sezione Single Sign-On Settings (Impostazioni Single Sign-On). Per ulteriori informazioni su ciascun privilegio, vedere la sezione "Amministrazione degli utenti" (Amministrazione degli utenti a pagina 22).

    Utilizzando account utente basati su directory, SSO tenta di ricevere solo i privilegi assegnati in questa sezione. Le impostazioni di directory Lights-Out non vengono applicate. Di seguito sono elencate le assegnazioni di privilegi predefinite:

  - Utente – Solo Login (Accesso)

- Operatore – Login (Accesso), Remote Console (Console remota), Power and Reset (Accensione e reimpostazione) e Virtual Media (Supporti virtuali)
- Amministratore – Login (Accesso), Remote Console (Console remota), Power and Reset (Accensione e reimpostazione), Virtual Media (Supporti virtuali), Configure iLO 2 (Configura iLO 2) e Administer Users (Amministra utenti)

- HP SIM Trusted Servers (Server attendibili HP SIM) – Consente di visualizzare lo stato dei server HP SIM attendibili configurati per l'uso di SSO con il processore LOM corrente. Fare clic su **Add a SIM Server** (Aggiungi server SIM) per aggiungere un nome di server, importare un certificato server o installare direttamente un certificato server. Per ulteriori informazioni, vedere la sezione "Aggiunta di server attendibili HP SIM" (Aggiunta di server attendibili HP SIM a pagina 56).

  Nella tabella dei server viene visualizzato l'elenco dei server HP SIM registrati con l'indicazione del relativo stato. Il numero effettivo di sistemi consentiti dipende dalla dimensione dei dati dei certificati memorizzati.

  Anche se un sistema è registrato, è possibile che SSO venga rifiutato a causa del livello di attendibilità o dello stato del certificato corrente. Ad esempio, se un nome di server HP SIM è registrato e il livello di attendibilità è impostato su Trust by Certificate (Considera attendibile per certificato), SSO non è consentito da tale server. Analogamente, se viene importato un certificato server HP SIM, ma questo è scaduto, SSO non è consentito da tale server. Inoltre, quando SSO è disabilitato, i record non vengono utilizzati. iLO 2 non impone la revoca dei certificati server SSO.

  - Status (Stato) – Indica lo stato del record (se sono presenti record installati).
  - Description (Descrizione) – Visualizza il nome del server (o soggetto del certificato). Una miniatura di certificato indica che il record contiene un certificato memorizzato.
  - Actions (Azioni) – Visualizza le azioni che è possibile eseguire su un record selezionato. Le azioni visualizzate dipendono dal tipo e dal numero di record installati:

    — Remove Name (Rimuovi nome) - Rimuove il record del nome del server.

    — Remove Certificate (Rimuovi certificato) - Rimuove il record del certificato.

Blocco del computer da console remota

La funzionalità di blocco del computer da console remota contribuisce alla protezione di un server gestito da iLO 2 bloccando il sistema operativo o effettuando la disconnessione di un utente in modo automatico nel momento in cui una sessione della console remota viene chiusa oppure si interrompe il collegamento tra iLO 2 e la rete. Diversamente dalla console remota o dalla console remota integrata, questa funzionalità viene fornita di serie e non richiede una licenza aggiuntiva. Di conseguenza, se si apre una finestra di sessione della console remota o della console remota integrata e questa funzionalità è configurata, il sistema operativo viene bloccato non appena la finestra viene chiusa, anche non sono state installate licenze aggiuntive.

È possibile visualizzare e configurare le impostazioni di blocco del computer da console remota tramite la scheda Administration (Amministrazione) o Remote Console (Console remota) nell'interfaccia di iLO 2. La funzionalità di blocco del computer da console remota è disabilitata per impostazione predefinita.

Per modificare le impostazioni della funzionalità di blocco del computer da console remota:

1. Accedere a iLO 2 usando un account che dispone del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).

2. Fare clic su **Administration>Security>Remote Console** (Amministrazione>Protezione>Console remota). Viene visualizzata la pagina Computer Lock Settings (Impostazioni blocco computer).

3. Modificare le impostazioni in base alle preferenze personali:

   ◦ Windows – Utilizzare questa opzione per configurare iLO 2 in modo da attivare la funzionalità di blocco su un server gestito con sistema operativo Windows®. Quando una sessione della console remota viene chiusa o si interrompe il collegamento tra iLO 2 e la rete, sul server viene automaticamente visualizzata la finestra di dialogo Computer Locked (Computer bloccato).

   ◦ Custom (Personalizzato) – Utilizzare questa opzione per configurare iLO 2 in modo da richiedere una sequenza di tasti personalizzata per bloccare un server gestito o disconnettere un utente collegato al server. Per definire la sequenza è possibile selezionare dall'elenco fino a cinque tasti. Quando una sessione della console remota viene chiusa o si interrompe il collegamento tra iLO 2 e la rete, la sequenza di tasti predefinita viene automaticamente inviata al sistema operativo del server.

   ◦ Disabled (Disabilitato) – Utilizzare questa opzione per disabilitare la funzionalità di blocco del computer da console remota. Nel momento in cui una sessione della console remota viene chiusa o si interrompe il collegamento tra iLO 2 e la rete, il server gestito non viene bloccato.

   Utilizzare i tasti elencati nella tabella riportata di seguito per creare la sequenza di tasti da associare alla funzione di blocco del computer da console remota.

ESC	F4	1	e
ALT-L	F5	2	f
ALT-R	F6	3	g
MAIUSC-L	F7	4	h
MAIUSC-R	F8	5	i
CTRL-L	F9	6	j
CTRL-R	F10	7	k
GUI-L	F11	8	l
GUI-R	F12	9	m
INS	" " (Barra spaziatrice)	:	n
CANC	!	;	o
HOME	"	<	p
FINE	#	=	q
PG_SU	$	>	r
PG_GIÙ	%	?	s
INVIO	&	@	t

<table>
<tr><td>TAB</td><td>'</td><td>[</td><td>u</td></tr>
<tr><td>BREAK</td><td>(</td><td>\</td><td>v</td></tr>
<tr><td>BACKSPACE</td><td>)</td><td>]</td><td>w</td></tr>
<tr><td>TASTNUM +</td><td>*</td><td>^</td><td>x</td></tr>
<tr><td>TASTNUM -</td><td>+</td><td>_</td><td>y</td></tr>
<tr><td>BLOC SCORR</td><td>,</td><td>'</td><td>z</td></tr>
<tr><td>R SIST</td><td>-</td><td>a</td><td>{</td></tr>
<tr><td>F1</td><td>.</td><td>b</td><td>}</td></tr>
<tr><td>F2</td><td>/</td><td>c</td><td>|</td></tr>
<tr><td>F3</td><td>0</td><td>d</td><td>~</td></tr>
</table>

4. Fare clic su **Apply** (Applica) per salvare le modifiche.

Questa funzionalità può essere configurata anche mediante scripting o righe di comando. Per ulteriori informazioni, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

Rete

Le schede Network Settings (Impostazioni di rete) e DCHP/DNS della sezione Network (Rete) consentono di visualizzare e modificare le impostazioni di rete di iLO 2.

Solo gli utenti che dispongono del privilegio Configure iLO 2 Settings (Configura impostazioni iLO 2) possono modificare queste impostazioni. Gli altri utenti potranno visualizzare solo le impostazioni assegnate.

Per modificare le impostazioni di rete per iLO 2:

1. Accedere a iLO 2 usando un account che dispone del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2). Fare clic su **Administration>Network** (Amministrazione>Rete).
2. Selezionare **Network Settings** (Impostazioni di rete) o **DHCP/DNS**.
3. Modificare le impostazioni nel modo necessario.
4. Dopo aver effettuato tutte le modifiche dei parametri, fare clic su **Apply** (Applica) per completare le modifiche.

iLO 2 viene riavviato e la connessione tra il browser e iLO 2 viene interrotta. Per ristabilire la connessione, attendere 60 secondi prima di avviare un'altra sessione del browser di effettuare l'accesso.

Impostazioni di rete

Nella pagina Network Settings (Impostazioni di rete) vengono visualizzati l'indirizzo IP del controller di rete, la maschera di sottorete e altre impostazioni relative al protocollo TCP/IP. Nell'omonima schermata è possibile abilitare o disabilitare DHCP e, nel caso di server che non utilizzano DHCP, configurare un indirizzo IP statico. Le impostazioni di rete sono visibili a tutti gli utenti, ma possono essere modificate soltanto dagli utenti che dispongono del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2). Per accedere alla pagina Network Settings (Impostazioni di rete), fare clic su

Administration>Network>Network (Amministrazione>Rete>Rete). La pagina Network Settings (Impostazioni di rete) viene visualizzata con le seguenti informazioni e impostazioni:

- L'opzione NIC consente di impostare il controller di rete di iLO 2 su Enabled (Abilitato), Disabled (Disabilitato) o Shared Network Port (Porta di rete condivisa).
    - Enabled (Abilitato) – Abilita l'interfaccia di rete di iLO 2 primaria.
    - Disabled (Disabilitato) – Disabilita l'interfaccia di rete di iLO 2. Per riabilitare l'interfaccia di rete, è necessario utilizzare l'utility RBSU di iLO 2 o un'altra utility di scripting basata su host.
    - Shared Network Port (Porta di rete condivisa) – Consente le connessioni di rete tramite la porta Ethernet dell'host specificato. La porta risulta come due indirizzi IP e MAC Ethernet separati sulla rete. Per ulteriori informazioni, vedere la sezione "Porta di rete condivisa iLO 2" (Porta di rete condivisa iLO 2 a pagina 63).
- L'opzione DHCP consente di selezionare un indirizzo IP statico (disabilitata) o utilizzare un server DHCP per ottenere un indirizzo IP per il sottosistema Integrated Lights-Out 2.

  Non è possibile impostare i parametri IP Address (Indirizzo IP iLO) e Subnet Mask (Maschera di sottorete) di iLO 2 se l'opzione DHCP è abilitata. Disabilitando questa opzione è possibile configurare l'indirizzo IP. Il campo IP Address (Indirizzo IP) è disponibile anche nella pagina DHCP/DNS Settings (Impostazioni DHCP/DNS). Se si modifica il valore del campo in una di queste due pagine, l'impostazione dell'opzione DHCP viene modificata.
- Il campo IP Address (Indirizzo IP) visualizza l'indirizzo IP di iLO 2. Se viene utilizzato il protocollo DHCP, l'indirizzo IP di iLO 2 viene fornito automaticamente. In caso contrario, immettere un indirizzo IP statico. Il campo IP Address (Indirizzo IP) è disponibile anche nella pagina DHCP/DNS. Se si immettono valori nel campo in una di queste due pagine, l'indirizzo IP di iLO 2 viene modificato.
- Il campo Subnet Mask (Maschera di sottorete) visualizza la maschera di sottorete della rete IP di iLO 2. Se viene utilizzato il protocollo DHCP, la maschera di sottorete viene fornita automaticamente. In caso contrario, immettere la maschera di sottorete per la rete.
- Il campo Gateway IP Address (Indirizzo IP gateway) visualizza l'indirizzo IP del gateway di rete. Se viene utilizzato il protocollo DHCP, l'indirizzo IP del gateway viene fornito automaticamente. In caso contrario, immettere l'indirizzo del gateway di rete.
- Il campo iLO 2 Subsystem Name (Nome sottosistema iLO 2) visualizza il nome utilizzato dal sottosistema iLO 2. Se DHCP e DNS sono configurati correttamente, è possibile utilizzare questo nome per connettersi al sottosistema iLO 2 in alternativa all'indirizzo IP. Per ulteriori informazioni, vedere la sezione "Limitazioni relative ai nomi del sottosistema iLO 2" (Limitazioni relative ai nomi del sottosistema iLO 2 a pagina 63).
- L'opzione Link (Collegamento) consente di controllare la velocità e il duplex del ricetrasmettitore di rete di iLO 2. È possibile evidenziare la velocità di collegamento corrente del controller di rete iLO 2 primario dedicato. Le impostazioni relative al collegamento comprendono:
    - Automatic (Automatico) (impostazione predefinita) consente a iLO 2 di negoziare i massimi valori supportati per velocità di collegamento e duplex durante la connessione alla rete.
    - 100Mb/FD impone una connessione a 100 Mb con full duplex.
    - 100Mb/HD impone una connessione a 100 Mb con half duplex.
    - 100Mb/FD impone una connessione a 10 Mb con full duplex.
    - 100Mb/HD impone una connessione a 10 Mb con half duplex.

    Se il rilevamento automatico è disabilitato, lo switch di rete deve far corrispondere le impostazioni di iLO 2 per evitare eventuali problemi di accesso.

Limitazioni relative ai nomi del sottosistema iLO 2

Il nome del sottosistema iLO 2 rappresenta il nome DNS del sottosistema iLO 2. Ad esempio, `iLO` anziché `iLO.hp.com`. Questo nome può essere utilizzato solo se il DHCP e DNS sono configurati correttamente in modo da effettuare la connessione al nome del sottosistema iLO 2 anziché all'indirizzo IP.

- Limitazioni del servizio nomi – Il nome del sottosistema viene utilizzato come parte del nome DNS e del nome WINS. Tuttavia le limitazioni relative ai nomi DNS e WINS sono diverse:
  - DNS consente di utilizzare caratteri alfanumerici e il trattino. WINS consente di utilizzare caratteri alfanumerici, il trattino e il carattere di sottolineatura.
  - I nomi del sottosistema WINS risultano troncati a 15 caratteri, quelli DNS no.

    Se è necessario inserire caratteri di sottolineatura, utilizzare l'utility RBSU o l'utility di scripting di iLO 2.

    NOTA: Le limitazioni del servizio nomi sono valide anche per il nome di dominio.

    Per evitare problemi legati allo spazio dei nomi:
  - Non utilizzare il carattere di sottolineatura.
  - Limitare i nomi del sottosistema a 15 caratteri.
  - Verificare che sia possibile eseguire il ping di iLO utilizzando l'indirizzo IP e il nome DNS/WIND.
  - Verificare che NSLOOKUP sia in grado di risolvere correttamente l'indirizzo di rete di iLO e che non siano presenti conflitti relativi allo spazio dei nomi.
  - Verificare che il DNS e WINS, se utilizzati entrambi, riescono a risolvere il nome, si utilizzati entrambi.
  - Allineare il nome DNS se si apportano modifiche allo spazio dei nomi.

Porta di rete condivisa iLO 2

La porta di rete condivisa iLO 2 consente di scegliere il controller di rete del sistema o il controller di rete di gestione iLO 2 dedicato per la gestione del server. Quando si abilita la porta di rete condivisa iLO 2, sia il normale traffico di rete sia quello destinato a iLO 2 passano attraverso il controller di rete del sistema.

iLO 2 fornisce il supporto per i server che non dispongono del controller di rete di gestione iLO 2 dedicato. Sui server in cui non è disponibile questo controller, la configurazione hardware standard fornisce la connettività di rete iLO 2 solo tramite la porta di rete condivisa. iLO 2 rileva la mancanza di un controller di rete di gestione iLO 2 dedicato e imposta automaticamente la porta di rete condivisa. Su alcuni di questi server, tuttavia, può essere disponibile un controller di rete di gestione iLO 2 dedicato come opzione hardware. In tal caso, iLO 2 utilizza per impostazione predefinita il controller di rete di gestione iLO 2 dedicato. Sui server in cui è utilizzato questo controller, è possibile abilitare la porta di rete condivisa tramite l'interfaccia di iLO 2.

Come porta di rete condivisa iLO 2 viene utilizzata la porta di rete NIC 1 sul pannello posteriore del server. La numerazione NIC nel sistema operativo può essere diversa da quella di sistema. La funzionalità della porta di rete condivisa iLO 2 non influisce sulle prestazioni di iLO 2. Il traffico di picco di iLO 2 è inferiore a 2 MB (in un controller di rete che supporta velocità pari a 1000 MB), ma il traffico medio raggiunge raramente i valori di picco.

La porta di rete condivisa non è disponibile sui server HP ProLiant ML310 G3, ML310 G4, BL20p G4 e su tutti i server blade c-Class.

Funzionalità e limitazioni della porta di gestione condivisa iLO 2

Per la gestione del server iLO 2 è possibile utilizzare solo la porta di rete condivisa iLO 2 e la porta del controller di rete di gestione iLO 2 dedicato. Queste due porte non possono funzionare contemporaneamente. Se si abilita il controller di rete di gestione iLO 2 dedicato, viene disabilitata la porta di rete condivisa iLO 2 e viceversa.

Tuttavia, la disabilitazione della porta di rete condivisa non disabilita completamente il controller di rete del sistema, attraverso il quale continua infatti a passare il normale traffico di rete. Quando il traffico relativo alla porta di rete condivisa è disabilitato, il traffico diretto o proveniente da iLO 2 non passa più da tale porta perché questa non è più condivisa con iLO 2.

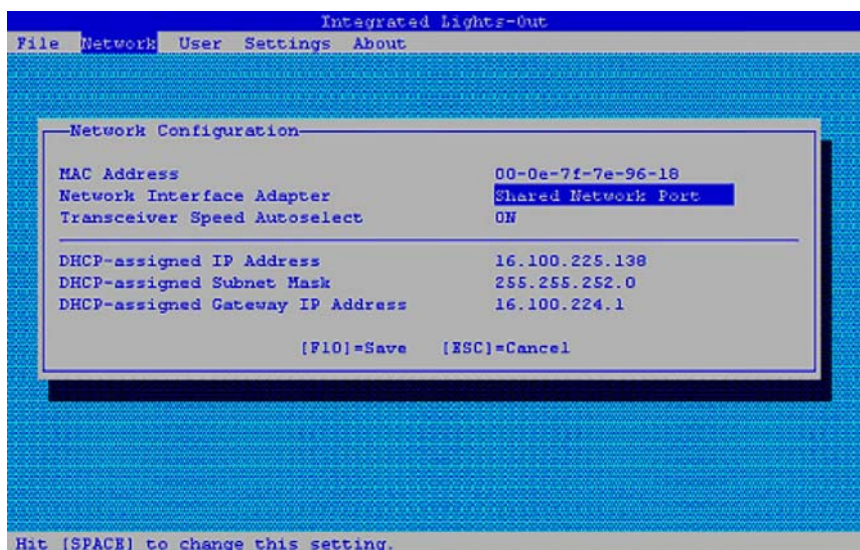
La porta di rete condivisa non deve essere considerata una funzione di disponibilità. Lo scopo della porta di rete condivisa è consentire il consolidamento delle porte di rete. L'utilizzo di questa funzionalità può creare un singolo punto di errore. In altri termini, se la porta genera un errore o viene scollegata dall'alimentazione esterna, sia l'host che iLO 2 non sono più disponibili sulla rete.

Abilitazione della funzionalità della porta di rete condivisa iLO 2

Per impostazione predefinita, la funzionalità della porta di rete condivisa iLO 2 è disabilitata. È possibile abilitarla e configurarla utilizzando gli elementi elencati di seguito:

- RBSU di iLO 2
- Interfaccia Web di iLO 2
- Script XML

Abilitazione della funzionalità della porta di rete condivisa iLO 2 tramite RBSU di iLO 2

1. Collegare la porta 1 del controller di rete del server a una rete LAN.
2. Alla richiesta del sistema durante il POST, premere il tasto **F8** per accedere all'RBSU di iLO 2.
3. Selezionare **Network>NIC>TCP/IP** (Rete>NIC>TCP/IP) e premere **Invio**.
4. Nel menu Network Configuration (Configurazione di rete), impostare il campo Network Interface Adapter (Scheda interfaccia di rete) su Shared Network Port (Porta di rete condivisa) premendo la barra spaziatrice. L'opzione Shared Network Port è disponibile solo sui server supportati.

5. Premere **F10** per salvare la configurazione.
6. Selezionare **File>Exit** (File>Esci) e premere **Invio**.

Dopo la reimpostazione di iLO 2 la porta di rete condivisa è attiva. Tutto il traffico di rete proveniente e destinato a iLO 2 viene diretto attraverso la porta 1 del controller di rete del sistema.

Abilitazione della funzionalità della porta di rete condivisa iLO 2 tramite interfaccia Web

1. Collegare la porta 1 del controller di rete iLO 2 a una rete LAN.
2. Avviare un browser e sfogliare fino all'indirizzo IP o al nome DNS di iLO 2.
3. Selezionare **Administration>Network Settings** (Amministrazione>Impostazioni di rete).
4. Nella pagina Network Settings (Impostazioni di rete), selezionare **Shared Network Port** (Porta di rete condivisa). La funzionalità relativa alla porta di rete condivisa è disponibile solo sui server supportati.
5. Fare clic su **Apply** (Applica) in fondo alla pagina.
6. Fare clic su **Yes** (Sì) nella finestra di dialogo di avviso, quindi su **OK**.

Dopo la reimpostazione di iLO 2 la porta di rete condivisa è attiva. Tutto il traffico di rete proveniente e destinato a iLO 2 viene diretto attraverso la porta 1 del controller di rete del sistema.

Per la gestione del server è attiva soltanto la porta di rete condivisa iLO 2 o la porta del controller di rete di gestione iLO 2 dedicato. Non è possibile abilitarle entrambe contemporaneamente.

Riabilitazione della porta di gestione iLO 2 dedicata

Per riabilitare la porta del controller di rete di gestione iLO 2 dedicato è necessario utilizzare l'interfaccia Web iLO 2, RBSU o gli script XML (descritto nella guida delle risorse mediante la riga di comando e lo scripting) Per riabilitare iLO 2 mediante RBSU è necessario riavviare il sistema.

Per riabilitare la porta del controller di rete di gestione iLO 2 dedicato tramite RBSU:

1. Collegare la porta del controller di rete di gestione iLO 2 dedicato a una rete LAN da cui è gestito il server.
2. riavviare il server.
3. Alla richiesta del sistema durante il POST, premere il tasto **F8** per accedere all'RBSU di iLO 2.
4. Selezionare **Network>NIC>TCP/IP** (Rete>NIC>TCP/IP) e premere **Invio**.
5. Nel menu Network Configuration (Configurazione di rete), impostare il campo Network Interface Adapter (Scheda interfaccia di rete) su ON premendo la barra spaziatrice.
6. Premere **F10** per salvare la configurazione.
7. Selezionare **File>Exit** (File>Esci) e premere **Invio**.

Una volta reimpostato iLO 2, la porta del controller di rete di gestione iLO 2 dedicato è attiva.

Per riabilitare la porta del controller di rete di gestione iLO 2 dedicato tramite l'interfaccia di iLO 2:

1. Avviare un browser e sfogliare fino all'indirizzo IP o al nome DNS di iLO 2.
2. Nella pagina Network Settings (Impostazioni di rete), impostare il controller di rete iLO 2 su **Enabled** (Abilitato).
3. Fare clic su **Apply** (Applica). Viene visualizzata una finestra di dialogo di avviso.
4. Fare clic su **Yes** (Sì), quindi su **OK**.

Una volta reimpostato iLO 2, il controller di rete di gestione iLO 2 dedicato è attivo. Quando si utilizza IRC tramite la porta del controller di rete di gestione iLO 2 dedicato, a seconda del traffico di rete è possibile che l'utente non abbia il tempo sufficiente per premere i tasti RBSU durante il POST.

Impostazioni DHCP/DNS

Nella pagina DHCP/DNS Settings (Impostazioni DHCP/DNS) di iLO 2 vengono visualizzate le informazioni di configurazione DHCP/DNS per iLO 2. Tutti gli utenti possono visualizzare le impostazioni DHCP/DNS, ma è necessario disporre del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2) per modificarle. Queste impostazioni possono essere modificate anche mediante l'utility RBSU di iLO 2 (premendo F8 durante il POST). Per accedere alle impostazioni DHCP/DNS, fare clic su **Administration>Network>DHCP/DNS** (Amministrazione>Rete>DHCP/DNS) Viene visualizzata la pagina DHCP/DNS Settings (Impostazioni DHCP/DNS).

Sono disponibili le opzioni riportate di seguito:

- L'opzione DHCP consente di selezionare un indirizzo IP statico (se disabilitata) o utilizzare un server DHCP per ottenere un indirizzo IP per il sottosistema iLO 2.

  Non è possibile impostare l'indirizzo IP di iLO 2 se l'opzione DHCP è abilitata. Disabilitando questa opzione è possibile configurare l'indirizzo IP. Il campo IP Address (Indirizzo IP) è disponibile anche nella pagina Network Settings (Impostazioni di rete). Se si modifica il valore del campo in una di queste due pagine, l'impostazione dell'opzione DHCP viene modificata.

- Il campo IP Address (Indirizzo IP) visualizza l'indirizzo IP di iLO 2. Se viene utilizzato il protocollo DHCP, l'indirizzo IP di iLO 2 viene fornito automaticamente. In caso contrario, immettere un indirizzo IP statico. Il campo IP Address (Indirizzo IP) è disponibile anche nella pagina Network Settings (Impostazioni di rete). Se si modifica il valore del campo in una di queste due pagine, l'indirizzo IP di iLO 2 viene modificato.

- Il campo Domain Name (Nome dominio) visualizza il nome del dominio in cui si trova il sottosistema iLO 2. Questo nome viene assegnato da DHCP (se il protocollo DHCP è abilitato). L'abilitazione del protocollo DHCP consente di configurare le seguenti opzioni DHCP:
    - Use DHCP Supplied Gateway (Usa gateway fornito da DHCP) – Consente di determinare se iLO 2 utilizzerà il gateway fornito dal server DHCP. In caso contrario, immettere un indirizzo di gateway nella casella Gateway IP Address (Indirizzo IP gateway).
    - Use DHCP Supplied DNS Servers (Usa server DNS forniti da DHCP) – Consente di determinare se iLO 2 utilizzerà l'elenco di server DNS forniti dal server DHCP. In caso contrario, immettere gli indirizzi dei server DNS nei campi relativi ai server DNS primario, secondario e terziario.
    - Use DHCP Supplied WINS Servers (Usa server WINS forniti da DHCP) – Consente di determinare se iLO 2 utilizzerà l'elenco di server WINS forniti dal server DHCP. In caso contrario, immettere gli indirizzi dei server WINS nei campi relativi ai server WINS primario e secondario.
    - Use DHCP Supplied Static Routes (Usa instradamenti statici forniti da DHCP) – Consente di determinare se iLO 2 utilizzerà gli instradamenti statici forniti dal server DHCP. In caso contrario, immettere l'indirizzo di instradamento statico nel campo Static Route #1, Static Route #2 o Static Route #3 (Instradamento statico #1, #2 o #3).
    - Use DHCP Supplied Domain Name (Usa nome dominio fornito da DHCP) – Consente di determinare se iLO 2 utilizzerà il nome di dominio fornito dal server DHCP. In caso contrario, immettere un nome di dominio nella casella Domain Name (Nome dominio).
- L'opzione WINS Server Registration (Registrazione server WINS) consente di determinare se iLO 2 registrerà il proprio nome con un server WINS.
- L'opzione DDNS Server Registration (Registrazione server DDNS) consente di determinare se iLO 2 registrerà il proprio nome con un server DDNS.
- L'opzione Ping Gateway on Startup (Esegui ping del gateway all'avvio) determina l'invio di quattro pacchetti di richieste echo ICMP al gateway durante l'inizializzazione di iLO 2. Questa opzione garantisce che la voce della cache ARP per iLO 2 risulti aggiornata sul router responsabile dell'instradamento dei pacchetti da e verso iLO 2.
- Il campo DHCP Server (Server DHCP) visualizza l'indirizzo IP del server DHCP. Questo campo non può essere assegnato. Viene ricevuto da DHCP, se il protocollo DHCP è abilitato, e rappresenta l'ultimo indirizzo di server DHCP noto valido.
- I campi Primary DNS Server, Secondary DNS Server e Tertiary DNS Server (Server DNS primario, secondario e terziario) visualizzano gli indirizzi IP dei server DNS. Se forniti dal server DHCP, i valori di questi campi vengono impostati automaticamente. In caso contrario, immettere gli indirizzi IP manualmente.
- I campi Primary WINS Server e Secondary WINS Server (Server WINS primario e secondario) visualizzano gli indirizzi IP dei server WINS. Se forniti dal server DHCP, i valori di questi campi vengono impostati automaticamente. In caso contrario, immettere gli indirizzi IP manualmente.
- I campi Static Route #1, Static Route #2 e Static Route #3 (destination, gateway) visualizzano gli indirizzi dei gateway di destinazione della rete. È possibile immettere al massimo tre coppie di instradamento gateway/destinazione della rete.

Impostazioni di SNMP/Insight Manager

L'opzione Management (Gestione) della sezione Administration (Amministrazione) consente di visualizzare la pagina SNMP/Insight Manager Settings (Impostazioni SNMP/Insight Manager).

L'opzione SNMP/Insight Manager Settings (Impostazioni SNMP/Insight Manager) consente la configurazione degli allarmi SNMP, la generazione di un allarme di prova e la configurazione dell'integrazione con HP SIM.

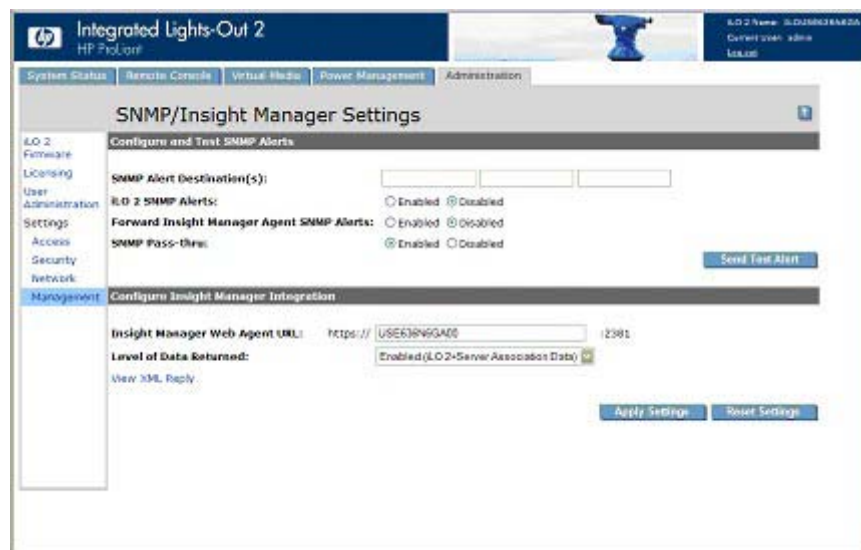
Abilitazione degli allarmi SNMP

Per la ricezione degli allarmi SNMP, iLO 2 supporta fino a tre indirizzi IP. In genere, viene utilizzato l'indirizzo IP della console del server di HP SIM (Systems Insight Manager).

Solo gli utenti che dispongono del privilegio Configure iLO 2 Settings (Configura impostazioni iLO 2) possono modificare queste impostazioni. Gli altri utenti potranno visualizzare solo le impostazioni assegnate.

La schermata SNMP/Insight Manager Settings (Impostazioni SNMP/Insight Manager) comprende le seguenti opzioni di allarme:

- SNMP Alert Destinations (Destinazioni allarmi SNMP)
- iLO 2 SNMP Alerts (Allarmi SNMP iLO 2)
- Forward Insight Manager Agent SNMP Alerts (Inoltra allarmi SNMP dell'agente di Insight Manager)
- SNMP pass-thru (Pass-through SNMP)
- p-Class Alert Fowarding (Inoltro allarmi p-Class) (visualizzato solo sui server p-Class)

Per ulteriori informazioni, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

Per configurare gli allarmi:

1. Accedere a iLO 2 usando un account che dispone del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).
2. Selezionare **Management** (Gestione) nella scheda Administration (Amministrazione). Viene visualizzata la schermata SNMP/Insight Manager Settings (Impostazioni SNMP/Insight Manager).
3. Nei campi SNMP Alert Destination(s) (Destinazioni allarmi SNMP) immettere fino a tre indirizzi IP come destinazione degli allarmi SNMP, quindi selezionare le opzioni di allarme che si desidera vengano supportate da iLO 2.
4. Fare clic su **Apply Settings** (Applica impostazioni).

I test relativi agli allarmi includono una trap di Insight Manager SNMP e vengono utilizzati per verificare la connessione di rete di iLO 2 in HP SIM. Solo gli utenti che dispongono del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2) possono inviare questo tipo di allarmi di prova.

Prima di eseguire un test degli allarmi, accertarsi di aver salvato le modifiche apportate ai campi SNMP Alert Destination(s) (Destinazioni allarmi SNMP).

Per inviare un allarme di prova:

1. Selezionare **Management** (Gestione) nella scheda Administration (Amministrazione). Viene visualizzata la schermata SNMP/Insight Manager Settings (Impostazioni SNMP/Insight Manager).
2. Fare clic su **Send Test Alert** (Invia allarme di prova) nella sezione Configure and Test SNMP Alerts (Configurazione e verifica allarmi SNMP) per generare un allarme di prova e inviarlo agli indirizzi TCP/IP salvati nei campi SNMP Alert Destinations (Destinazioni allarmi SNMP).
3. Una volta generato l'allarme, verrà visualizzata una finestra di conferma.
4. Controllare la ricezione della trap nella console di HP SIM.

Definizioni di trap generati da SNMP

È possibile generare i seguenti trap SNMP sui server BL c-Class e iLO 2:

- ALERT_TEST consente di verificare il corretto funzionamento della configurazione SNMP, della console SNMP client e della rete. È possibile utilizzare l'interfaccia di iLO 2 per la generazione di questo allarme in modo da verificare la ricezione dell'allarme sulla console SNMP. È inoltre possibile generare questo allarme utilizzando la ROM opzionale di iLO 2 per verificare le impostazioni di configurazione SNMP.
- ALERT_SERVER_POWER viene generato quando il processore di gestione iLO 2 rileva una transizione imprevista dell'alimentazione del sistema host, ossia da ON a OFF oppure da OFF a ON. Per transizioni impreviste dell'alimentazione del sistema host si intendono cambiamenti dovuti a eventi sconosciuti al processore di gestione. Questo allarme non viene generato quando il sistema viene acceso o spento mediante l'interfaccia di iLO 2, CLI, RIBCL o altre funzionalità di gestione. Se il sistema viene spento a causa del sistema operativo, per effetto della pressione del pulsante di accensione o per altri motivi, l'allarme viene generato e inviato.
- ALERT_SERVER_RESET viene generato quando il processore di gestione iLO 2 viene utilizzato per eseguire un avvio a freddo o un avvio a caldo del sistema host. Viene inoltre inviato quando il processore di gestione iLO 2 rileva che il sistema host è in fase di reimpostazione a causa di eventi sconosciuti. Determinati comportamenti e azioni del sistema operativo possono determinare il rilevamento di questo tipo di evento e, di conseguenza, la trasmissione dell'allarme.
- ALERT_ILLEGAL_LOGIN è un allarme SNMP trasmesso quando viene effettuato un tentativo di connessione con nome utente e password non validi. Questo allarme viene trasmesso indipendentemente dal tipo di connessione, interfaccia Web, porta seriale, Telnet, SSH o RIBCL.
- ALERT_LOGS_FULL è un allarme SNMP trasmesso quando il registro eventi di iLO 2 è pieno e viene effettuato un tentativo di registrazione di un nuovo evento.
- ALERT_SELFTEST_FAILURE è un allarme SNMP trasmesso quando iLO 2 rileva un errore in uno qualsiasi dei componenti interni monitorati. In caso di rilevamento di errore, viene trasmesso un allarme SNMP.
- ALERT_SECURITY_ENABLED viene trasmesso quando il processore di gestione iLO 2 rileva l'abilitazione dell'interruttore di esclusione della protezione.

- ALERT_SECURITY_DISABLED viene trasmesso quando il processore di gestione iLO 2 rileva la disabilitazione dell'interruttore di esclusione della protezione.
- ALERT_HOST_GENERATED viene generato quando al processore di gestione iLO 2 è stato richiesto di trasmettere un allarme host (pass-through SNMP), ma il processore non è riuscito a trasmettere l'allarme SNMP originale. iLO 2 tenta di trasmettere questo allarme generico per notificare alla console di gestione SNMP la mancata trasmissione di un allarme dal sistema host.

Configurazione dell'integrazione di Insight Manager

L'opzione Insight Manager Web Agent URL (URL agente Web di Insight Manager), nome DNS o indirizzo IP, consente di impostare la destinazione del collegamento Insight Agent sulle pagine di iLO 2. In genere, questo collegamento corrisponde all'indirizzo IP o al nome DNS dell'agente di gestione in esecuzione sul sistema operativo del server host.

Immettere l'indirizzo IP del server host. Il protocollo (https://) e il numero di porta (:2381) vengono aggiunti automaticamente all'indirizzo IP o al nome DNS per consentire l'accesso agli agenti Web di Insight Management da iLO 2.

Se l'opzione Insight Manager Web Agent URL (URL agente Web di Insight Manager) viene impostata utilizzando un altro metodo, ad esempio CPQLOCFG, scegliere il pulsante di aggiornamento del browser per visualizzare l'URL aggiornato.

L'impostazione Level of Data Returned (Livello di dati restituiti) consente di controllare il contenuto di un messaggio anonimo ricevuto da iLO 2. Le informazioni restituite vengono utilizzate per le richieste di identificazione HTTP di Insight Manager. Sono disponibili le opzioni riportate di seguito:

- Enabled (Abilitato) – Si tratta dell'impostazione predefinita e consente a Insight Manager di associare il processore di gestione al server host. Fornisce dati sufficienti per permettere l'integrazione con HP SIM.
- Disabled (Disabilitato) – Impedisce a iLO 2 di rispondere alle richieste di HP SIM.
- View XML (Visualizza risposta XML) – Consente di esaminare i dati restituiti in base alle impostazioni.

  Viene visualizzata la risposta che verrà restituita a Insight Manager quando quest'ultimo richiede l'identificazione del processore di gestione utilizzando questo collegamento.

Per visualizzare i risultati delle modifiche apportate, salvare queste ultime facendo clic su **Apply Settings** (Applica impostazioni). Fare clic su **Reset Settings** (Reimposta impostazioni) per eliminare il contenuto dei campi e riportare la pagina allo stato originale. Il pulsante Reset Settings (Reimposta impostazioni) non consente di salvare tutte le modifiche.

Per ulteriori informazioni su Insight Agents, fare clic su **System Status>Insight Agent** (Stato del sistema>Insight Agent).

Configurazione del server ProLiant BL p-Class

Per accedere ai server ProLiant BL p-Class ed eseguirne la configurazione, è possibile usare:

- Porta di diagnostica di iLO 2 situata nella parte anteriore del server.
- Configurazione basata sul browser (Impostazione di iLO 2 mediante l'opzione basata su browser a pagina 13), che determina la configurazione iniziale del sistema tramite la porta di diagnostica di iLO 2.
- Installazione guidata dettagliata mediante l'installazione di HP BladeSystem.

In alcuni server blade p-Class, installati in contenitori con backplane di gestione aggiornati che supportano blade ad alta densità, è possibile usare iLO 2 per configurare l'indirizzo IP statico iniziale per il contenitore. La configurazione iniziale del server blade nell'alloggiamento 1 permette di assegnare a tutti gli iLO 2 successivi del contenitore indirizzi IP statici predefiniti. Questa funzione è supportata da iLO 1.55 e versioni successive.

Requisiti per gli utenti del server ProLiant BL p-Class

- Gli utenti devono disporre del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).
- Deve essere disponibile e funzionante una connessione di rete per iLO 2.

Configurazione degli alloggiamenti con IP statico

La configurazione degli alloggiamenti con IP statico viene implementata mediante l'opzione Static IP Bay Settings (Impostazioni alloggiamenti con IP statico) disponibile nella scheda BL p-Class. Questa opzione consente di facilitare la distribuzione iniziale di un intero contenitore o la successiva installazione di server blade all'interno di un contenitore esistente. Anche se il metodo preferito per l'assegnazione degli indirizzi IP al processore iLO 2 nei singoli server blade rimane quello basato su DHCP e DNS, questi protocolli non sono sempre disponibili sulle reti di prova.

Ad esempio, dopo la configurazione dell'alloggiamento con IP statico per il blade dell'alloggiamento 1, agli eventuali altri blade aggiunti nel contenitore verranno assegnati indirizzi successivi senza DHCP. Gli indirizzi di rete vengono assegnati in base alla posizione del blade nell'alloggiamento 1: 192.168.1.1, alloggiamento 2: 192.168.1.2 e così via. L'implementazione di blade successivi non richiede operazioni di configurazione aggiuntive e gli indirizzi di rete corrispondono al numero dell'alloggiamento.

La configurazione degli alloggiamenti con IP statico automatizza la prima fase della procedura di implementazione di server blade BL p-Class abilitando il processore di gestione iLO 2 in ogni alloggiamento blade, in modo da ottenere un indirizzo IP predefinito senza dover utilizzare il protocollo DHCP. iLO 2 è immediatamente accessibile per l'implementazione del server tramite Virtual Media (Supporti virtuali) e altre funzionalità di gestione remota.

La configurazione degli alloggiamenti con IP statico utilizza il metodo di indirizzamento Static IP Bay Configuration (Configurazione alloggiamenti con IP statico), che permette di assegnare un indirizzo IP a ogni iLO 2 in base alla posizione dell'alloggiamento nel relativo contenitore server. Fornendo un insieme di indirizzi IP per tutto il contenitore, si può disporre dei vantaggi offerti dalla configurazione degli alloggiamenti con IP statico, senza dover configurare localmente ogni singolo iLO 2.

Questo tipo di configurazione offre i seguenti vantaggi:

- Permette di evitare i costi di un'infrastruttura DHCP per supportare l'ambiente blade.
- Semplifica la procedura di installazione generando automaticamente indirizzi iLO 2 per tutti gli alloggiamenti o solo per quelli selezionati.

La configurazione degli alloggiamenti con IP statico non è supportata nei contenitori blade G1 BL-series. Per visualizzare la generazione del contenitore, fare clic su **BL p-Class>Rack View>Details** (BL p-Class>Visualizzazione rack>Dettagli) in modo da visualizzare i dettagli relativi a un contenitore specifico. La configurazione degli alloggiamenti con IP statico non è supportata su un contenitore quando nei dettagli relativi al tipo di contenitore viene visualizzato il messaggio `BL Enclosure G1` (BL contenitore G1).

Quando si esegue di nuovo l'implementazione di un blade, è possibile che la configurazione degli alloggiamenti con IP statico non sia completa. Per risolvere il problema, verificare che il blade utilizzi il firmware di iLO 2 corrente, quindi ripristinare le impostazioni predefinite di iLO 2 mediante l'utility RBSU.

Configurazione di un contenitore di tipo blade ProLiant BL p-Class

Per configurare un contenitore di tipo blade BL p-Class mediante l'indirizzamento degli IP statici degli alloggiamenti:

1. Installare un server blade nell'alloggiamento 1 del contenitore del BL p-Class. Non è necessario che il server blade sia configurato o che abbia un sistema operativo installato. Il server blade deve essere configurato prima di installare nel contenitore altri blade.
2. Collegare un'unità client alla porta iLO 2 del pannello frontale del blade tramite il cavo di I/O locale. Il cavo di I/O locale si collega alla porta di I/O che si trova nella parte anteriore del server blade. Questa connessione permette di assegnare l'indirizzo IP statico 192.168.1.1 all'interfaccia Web di iLO 2.
3. Configurare le impostazioni del contenitore. Tramite l'interfaccia Web di iLO 2, selezionare la scheda BL p-Class per accedere alle impostazioni degli IP statici del contenitore. La scheda BL p-Class comprende un'interfaccia utente per la configurazione degli indirizzi IP statici a livello del contenitore.
4. Selezionare un indirizzo IP iniziale adeguato, le cui ultime cifre corrispondano al numero di alloggiamento di ogni blade (ad esempio: da 192.168.100.1 a 192.168.100.16), per creare un sistema di numerazione facile da ricordare.
5. Se necessario reimpostare l'alloggiamento n°1. Il blade presente nell'alloggiamento 1 deve essere reimpostato soltanto se si desidera abilitare un indirizzo IP statico di configurazione dell'alloggiamento per il blade selezionando l'opzione di abilitazione della maschera per l'alloggiamento 1. Prima di riavviare il server blade, aprire la pagina Network Settings (Impostazioni di rete), selezionare **Enable Static IP Settings** (Abilita impostazioni IP statici), quindi fare clic su **Apply** (Applica) per forzare il riavvio del server e utilizzare l'indirizzo IP statico appena assegnato al contenitore.

Se si installano contemporaneamente più contenitori, la procedura può essere facilmente ripetuta spostando un singolo server nell'alloggiamento 1 di ogni contenitore per eseguire la configurazione.

Configurazione degli alloggiamenti con IP statico

Le impostazioni degli alloggiamenti con IP statico disponibili nella scheda BL p-Class consentono di configurare e di installare il server blade. Quando si configurano queste impostazioni, è necessario utilizzare il blade presente nell'alloggiamento 1.

La casella di controllo Enable Static IP Bay Configuration Settings (Abilita impostazioni configurazione alloggiamenti con IP statico), disponibile nella scheda Network Settings (Impostazioni di rete), non illustrata, permettono di abilitare e di disabilitare l'opzione Static IP Bay Configuration (Configurazione alloggiamenti con IP statico). La nuova opzione Enable Static IP Bay Configuration Settings (Abilita impostazioni configurazione alloggiamenti con IP statico) è disponibile solo per i server blade. Quando l'opzione Static IP Bay Configuration (Configurazione alloggiamenti con IP statico) è abilitata, tutti i campi ad eccezione di iLO 2 Subsystem Name (Nome sottosistema iLO 2) sono disabilitati. In un momento specifico può essere attiva solo l'opzione Static IP Bay Configuration (Configurazione alloggiamenti con IP statico) o l'opzione DHCP. Disabilitando Static IP Bay Configuration (Configurazione alloggiamenti con IP statico) e DHCP si segnala a iLO 2 di utilizzare un indirizzo IP definito dall'utente. L'opzione Enable Static IP Bay Configuration Settings (Abilita impostazioni configurazione alloggiamenti con IP statico) rimane disabilitata se l'infrastruttura non supporta Static IP Bay Configuration (Configurazione alloggiamenti con IP statico).

Parametri di configurazione standard per ProLiant BL p-Class

Beginning IP Address (Bay 1) (Indirizzo IP iniziale (alloggiamento 1)) – Assegna l'indirizzo IP iniziale. Tutti gli indirizzi IP devono essere indirizzi validi.

Ending IP Address (Bay 16) (Indirizzo IP finale (alloggiamento 16)) – Assegna l'indirizzo IP finale. Tutti gli indirizzi IP devono essere indirizzi validi.

Subnet Mask (Maschera di sottorete) - Assegna la maschera di sottorete per il gateway predefinito. Questo campo può essere completato se è abilitata l'opzione Static IP Bay Configuration (Configurazione alloggiamenti con IP statico) o l'opzione DHCP. L'intero campo di indirizzi IP deve essere conforme alla maschera di sottorete.

Gateway IP Address (Indirizzo IP gateway) - Assegna l'indirizzo IP del router di rete che collega la sottorete di Remote Insight a un'altra sottorete nella quale risiede il PC di gestione. Questo campo può essere completato se è abilitata l'opzione Static IP Bay Configuration (Configurazione alloggiamenti con IP statico) o l'opzione DHCP.

Parametri di configurazione avanzati per ProLiant BL p-Class

Domain Name (Nome dominio) - Assegna il nome del dominio di cui farà parte iLO 2.

Primary DNS Server (Server DNS primario) - Assegna un indirizzo IP univoco di server DNS sulla rete.

Secondary DNS Server (Server DNS secondario) - Assegna un indirizzo IP univoco di server DNS sulla rete.

Tertiary DNS Server (Server DNS terziario) - Assegna un indirizzo IP univoco di server DNS sulla rete.

Primary WINS Server (Server WINS primario) - Assegna un indirizzo IP univoco di server WINS sulla rete.

Secondary WINS Server (Server WINS secondario) - Assegna un indirizzo IP univoco di server WINS sulla rete.

Static Route #1, #2, and #3 (destination gateway) (Percorso statico 1, 2 e 3 (gateway di destinazione)) - Assegna la destinazione di instradamento statico appropriata e un indirizzo IP al gateway sulla rete (i

valori IP predefiniti sono 0.0.0.0 e 0.0.0.0, dove il primo indirizzo corrisponde all'IP di destinazione e il secondo corrisponde all'IP del gateway).

Abilitazione dell'assegnazione di un indirizzo IP a iLO 2

Le caselle corrispondenti agli alloggiamenti da 1 a 16 consentono di selezionare i server di tipo blade BL p-Class da configurare. È possibile scegliere tra Enable All (Abilita tutto), Clear All (Cancella tutto) o Apply (Applica) la selezione.

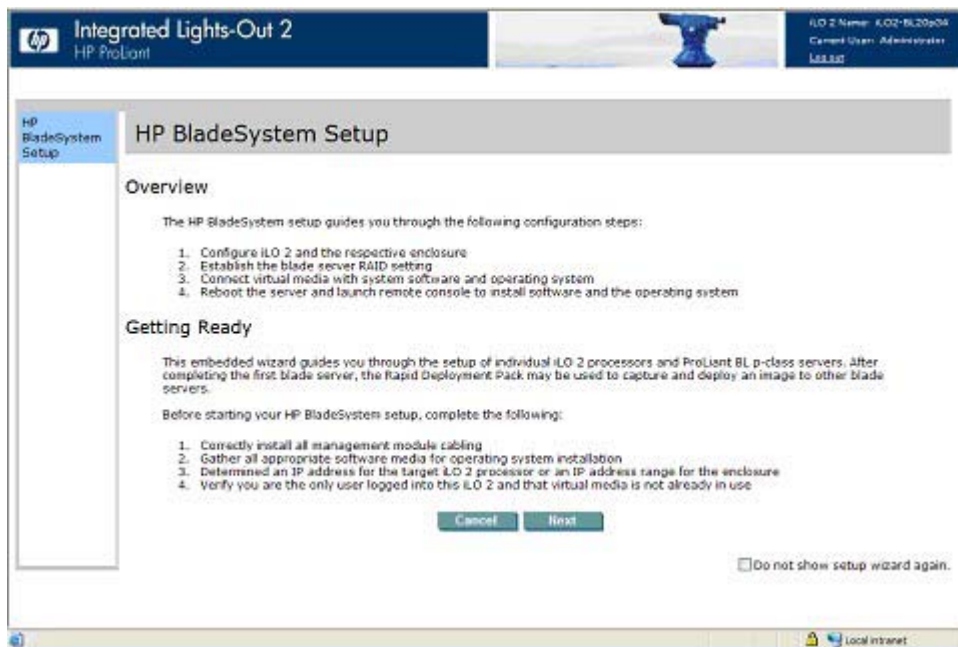
Installazione di HP BladeSystem

L'installazione guidata di HP BladeSystem fornisce istruzioni dettagliate per semplificare la configurazione di un solo blade senza dover usare DHCP o PXE. La pagina dell'installazione di HP BladeSystem viene visualizzata dopo avere eseguito l'autenticazione di iLO 2 mediante la porta anteriore.

Il server blade deve essere collegato correttamente per la connettività iLO 2. Collegare il server blade tramite la porta I/O del server, mentre il blade si trova nel rack. Questo metodo richiede di collegare il cavo I/O locale alla porta I/O e a un PC client. Usando l'indirizzo IP statico riportato sull'etichetta del cavo I/O e le informazioni iniziali di accesso che si trovano nella parte anteriore del server blade, è possibile accedere al server blade mediante iLO 2 tramite l'interfaccia del browser Web standard.

Benché per l'accesso sia possibile usare qualsiasi blade, se per configurare le impostazioni di rete di iLO 2 si utilizza la configurazione degli alloggiamenti con IP statico, è necessario utilizzare per l'accesso il primo blade del contenitore.

La prima pagina dell'installazione guidata viene visualizzata automaticamente nei seguenti casi:

- L'installazione riguarda un nuovo blade ed è stato eseguito l'accesso a iLO 2 mediante la porta anteriore.
- L'installazione guidata non è stata interamente completata scegliendo **Finish** (Fine) nell'ultima pagina e non sono state selezionate le opzioni **Do not show setup wizard again** (Non mostrare più l'installazione guidata) e **Cancel** (Annulla) nella pagina iniziale.
- Sono state ripristinate le impostazioni predefinite di iLO 2.

Fare clic su **Cancel** (Annulla) per chiudere l'installazione guidata automatica. Fare clic su **Next** (Avanti) per configurare il server blade. L'installazione guidata consente di eseguire le seguenti operazioni:

1. Configurazione di iLO 2
2. Verifica RAID del server
3. Collegamento dei supporti virtuali
4. Installazione del software

Schermata di configurazione di iLO 2

Questa schermata consente di modificare le seguenti impostazioni:

- Password amministratore. HP consiglia di modificare la password predefinita.
- Impostazioni configurazione di rete. Di seguito sono riportate le impostazioni predefinite:
    - Enable DHCP (Abilita DHCP): Yes (Sì)
    - Enable Static IP Bay Configuration (Abilita impostazioni configurazione alloggiamenti con IP statico): No
- In caso di collegamento al blade nell'alloggiamento 1 del contenitore, è possibile abilitare la configurazione degli alloggiamenti IP statici in modo da preconfigurare l'indirizzo statico per gli altri processori iLO 2 del contenitore.

Nella configurazione predefinita, al processore iLO 2 in fase di aggiornamento viene assegnato l'indirizzo IP tramite DHCP. Gli altri processori iLO 2 del contenitore devono essere configurati separatamente. Se queste impostazioni non vengono modificate e si fa clic su **Next** (Avanti), viene visualizzata la pagina successiva dell'installazione guidata. Se almeno una delle suddette impostazioni viene modificata, iLO 2 viene riavviato per rendere effettive le impostazioni aggiornate.

Sono inoltre disponibili le seguenti combinazioni di configurazioni (le impostazioni predefinite sono indicate tra parentesi):

- Enable DHCP (Abilita DHCP): Yes (Sì) e Enable Static IP Bay Configuration (Abilita impostazioni configurazione alloggiamenti con IP statico): Yes (Sì)

  In questa configurazione, al processore iLO 2 in fase di configurazione viene assegnato l'indirizzo IP tramite DHCP. Se si fa clic su **Next** (Avanti) viene visualizzata la pagina Static IP Bay Configuration (Configurazione alloggiamenti con IP statico), che consente di specificare gli indirizzi IP per gli altri processori iLO 2 del contenitore. Una volta selezionato **Next** (Avanti), viene chiesto di confermare l'utilizzo di DHCP per l'indirizzo IP di questo processore iLO 2.

- Enable DHCP (Abilita DHCP): No e Enable Static IP Bay Configuration (Abilita impostazioni configurazione alloggiamenti con IP statico): Yes (Sì)

  Mediante questa configurazione, l'indirizzo IP del processore iLO 2 viene impostato in base alle impostazioni specificate tramite la configurazione degli alloggiamenti con IP statico. Se si fa clic su **Next** (Avanti) viene visualizzata la pagina Static IP Bay Configuration (Configurazione alloggiamenti con IP statico).

- Enable DHCP (Abilita DHCP): No e Enable Static IP Bay Configuration (Abilita impostazioni configurazione alloggiamenti con IP statico): No

  Mediante questa configurazione, l'indirizzo IP del processore iLO in fase di configurazione viene impostato in base alle impostazioni specificate tramite la pagina Network Settings (Impostazioni di rete). Se si fa clic su **Next** (Avanti) viene visualizzata la pagina Network Settings (Impostazioni di rete).

Per poter salvare le modifiche apportate alle impostazioni di rete, è necessario disporre del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2).

Fare clic su **Next** (Avanti) per salvare le modifiche e continuare.

Schermata Verify Server RAID Configuration

Questo passaggio dell'installazione guidata consente di verificare e accettare le impostazioni della configurazione RAID del server. Verificare il livello RAID rilevato per le unità disco rigido del server blade visualizzato sulla pagina Web, quindi effettuare una delle seguenti operazioni:

- Fare clic su **Next** (Avanti) per mantenere le impostazioni RAID correnti.
- Fare clic su **Default Settings** (Impostazioni predefinite) per configurare automaticamente il livello RAID in base al numero di unità installate. Verrà richiesto di confermare che si intende reimpostare il livello RAID, dal momento che ciò potrebbe provocare la perdita di dati. Per reimpostare i livelli RAID è necessario accendere o riavviare il server. In iLO 2 viene visualizzata una pagina che indica l'esecuzione dell'operazione. La pagina viene aggiornata automaticamente ogni 10 secondi. Una volta riavviato il server, viene visualizzata di nuovo la pagina successiva dell'installazione guidata. Se si verifica un errore durante il processo di reimpostazione del RAID, vengono visualizzati di nuovo la pagina di configurazione RAID e il messaggio di errore. È più probabile che si verifichi un errore se il server è in POST. In questo caso, chiudere i programmi RBSU in esecuzione, consentire il completamento della procedura POST ed eseguire di nuovo l'operazione.

È possibile modificare manualmente il livello RAID tramite RBSU. Se il sistema operativo è già installato, la modifica del livello RAID provoca la perdita di dati.

Schermata Connect Virtual Media

Questo passaggio dell'installazione guidata consente di verificare e accettare l'unità da usare durante l'installazione del sistema operativo. Nella sezione Settings (Impostazioni), selezionare l'unità locale e il tipo di supporto che si intende usare durante l'installazione del sistema operativo. Fare clic su **Launch Virtual Media** (Avvia supporto virtuale) per avviare l'applet Virtual Media.

- Verificare che il supporto del sistema operativo sia collegato. Nell'applet Virtual Media verrà visualizzata un'icona verde accanto al supporto selezionato.
- Verificare che il supporto del sistema operativo si trovi nell'unità locale appropriata.
- Accettare i certificati di protezione visualizzati.

Dopo avere effettuato la selezione, fare clic su **Next** (Avanti) per salvare le impostazioni e continuare. Viene visualizzato l'applet Virtual Media. Una volta che l'applet è disponibile, è possibile modificare l'unità selezionata o scegliere altre opzioni non disponibili dalla pagina di installazione guidata.

Schermata Install Software

Questo passaggio dell'installazione guidata consente di avviare la console remota e installare il sistema operativo. Per iniziare il processo di installazione del sistema operativo:

- Fare clic su **Launch Software Installation** (Avvia installazione software) per avviare la console remota. iLO 2 esegue automaticamente l'accensione o il riavvio del server per avviare l'installazione del sistema operativo mediante il supporto virtuale precedentemente selezionato.
- Accettare i certificati di protezione visualizzati.

Fare clic su **Finish** (Fine) per completare il processo di configurazione.

Parametri di configurazione della porta di diagnostica iLO 2

La porta di diagnostica di iLO 2, disponibile nella parte anteriore dei server ProLiant BL classe P, consente di accedere al server e di risolvere i relativi problemi mediante un cavo diagnostico. La porta di diagnostica di iLO 2 utilizza un indirizzo IP statico. Non ricorre a DHCP per ottenere un indirizzo IP, eseguire la registrazione su WINS o DDNS o usare un gateway. Il cavo della porta di diagnostica non deve essere collegato senza che vi sia una connessione di rete attiva, poiché ciò causerebbe la diminuzione delle prestazioni della rete sulla porta di rete iLO 2 standard.

In Network Settings (Impostazioni di rete) è possibile configurare le informazioni specifiche della porta di diagnostica. Per ulteriori informazioni sull'uso della porta di diagnostica e del relativo cavo, consultare la Guida all'installazione e alla configurazione del server blade.

Di seguito sono elencati i campi di configurazione disponibili per la porta di diagnostica:

- Enable NIC (Abilita controller di rete)

  Se l'opzione Enable NIC (Abilita scheda di rete) è impostata su Yes (Sì), la porta di diagnostica è abilitata.

- Transceiver Speed Autoselect (Selezione automatica velocità ricetrasmettitore)
- Velocità
- Duplex
- Indirizzo IP

  Questo parametro consente di assegnare a iLO 2 un indirizzo IP statico della rete. Per impostazione predefinita, l'indirizzo IP viene assegnato dal protocollo DHCP. Per impostazione predefinita, l'indirizzo IP è 192.168.1.1 per tutte le porte di diagnostica di iLO 2.

- Maschera di sottorete
  - Questo parametro consente di assegnare la maschera di sottorete alla porta di diagnostica di iLO 2. Per impostazione predefinita la maschera di sottorete è 255.255.255.0 per tutte le porte di diagnostica di iLO 2.
  - L'uso della porta di diagnostica viene rilevato automaticamente quando si collega un cavo di rete attivo. Quando si effettua la commutazione tra le porte posteriori e quella di diagnostica, è necessario attendere 90 secondi affinché il processo di commutazione della rete si concluda prima di tentare una nuova connessione attraverso il browser Web.

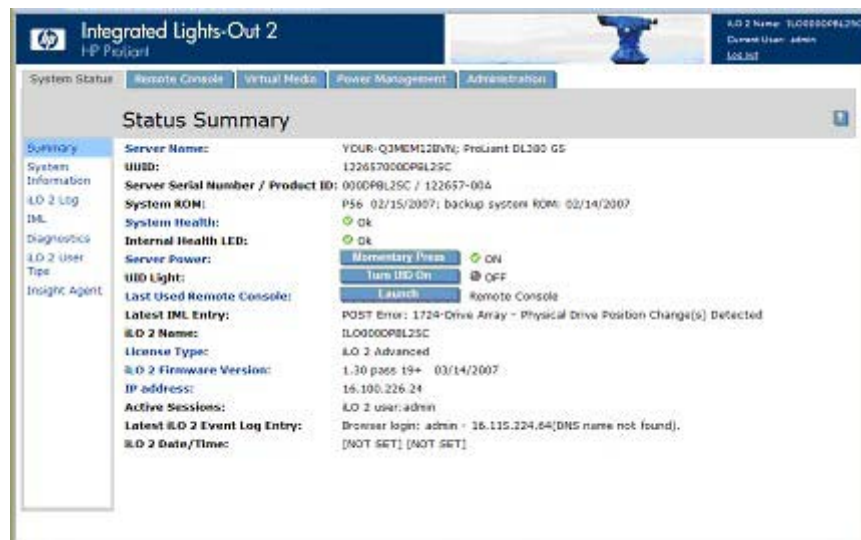
  NOTA: Se è attiva una sessione della console remota o è in corso l'aggiornamento del firmware, la porta di diagnostica non effettuerà la commutazione.

4 Utilizzo di iLO 2

In questa sezione

Stato del sistema e informazioni di riepilogo sullo stato del sistema

Quando si accede per la prima volta a iLO 2 viene visualizzata la pagina Status Summary (Riepilogo dello stato) in cui sono riportati lo stato del sistema e le informazioni di riepilogo sullo stato. In questa pagina viene inoltre fornito l'accesso a informazioni sulla sicurezza, ai registri di sistema e a informazioni Insight Agent. Le opzioni disponibili nella sezione System Status (Stato sistema) sono: Summary (Riepilogo), System Information (Informazioni di sistema), iLO 2 Log (Registro di sistema iLO 2), IML, Diagnostics (Diagnostica), iLO 2 User Tips (Suggerimenti per l'utilizzo di iLO 2) e Insight Agents.

Nella pagina Status Summary (Riepilogo dello stato) vengono visualizzate informazioni estremamente dettagliate relative al sistema e al sottosistema iLO 2. Sono inoltre disponibili collegamenti alle funzionalità di utilizzo più frequente. Per accedere alla pagina Status Summary (Riepilogo dello stato) da altre aree dell'interfaccia di iLO 2, fare clic su **System Status>Summary** (Stato sistema>Riepilogo).

Le informazioni sullo stato includono:

- Server Name (Nome server) - Nome del server. Fornisce inoltre un collegamento a Administration>Options>Access (Amministrazione>Opzioni>Accesso).
- UUID - ID del server.
- Server Serial Number/Product ID (Numero di serie del server/ID prodotto) – Numero di serie del server assegnato dalla casa produttrice. Questo numero di serie può essere modificato mediante l'utility RBSU del sistema durante il POST. L'ID del prodotto consente di distinguere sistemi differenti con numeri di serie simili. Sebbene sia assegnato dalla casa produttrice, l'ID del prodotto può essere modificato mediante l'utility RBSU del sistema durante il POST.
- System ROM (ROM di sistema) – Famiglia e versione della ROM di sistema attiva. Se il sistema supporta una ROM per il backup, viene visualizzata anche la data del backup.
- System Health (Sicurezza del sistema) - Riepilogo delle condizioni dei sottosistemi monitorati tra cui lo stato generale e il livello di ridondanza (capacità di gestire un guasto). Fornisce inoltre un collegamento a System>Status>System Information Summary (Sistema>Stato>Riepilogo delle informazioni di sistema).
- Internal Health LED (LED sicurezza interna) – Indicatore di sicurezza interna del server (se supportato). Consente di visualizzare un riepilogo degli eventuali problemi relativi a ventole, sensori di temperatura, VRM e altri sottosistemi server che è necessario monitorare. Per ulteriori informazioni, vedere la sezione "Riepilogo delle informazioni di sistema" (Riepilogo delle informazioni di sistema a pagina 80).
- TPM Status (Stato TPM) - Stato della configurazione TPM. Se il sistema host o la ROM di sistema non supporta la funzionalità TPM, nella pagina Status Summary (Riepilogo dello stato) non viene visualizzato lo stato TPM. Per ulteriori informazioni, vedere la sezione "Supporto Trusted Platform Module".
- Server Power (Alimentazione server) - Stato di alimentazione del server (ON/STANDBY) nel momento in cui è stata caricata la pagina. Fornisce inoltre un collegamento a Server>Power Management (Server>Gestione alimentazione). Gli utenti che dispongono del privilegio Virtual Power and Reset (Accensione virtuale e reimpostazione) possono utilizzare anche il pulsante Momentary Press (Pressione momentanea).
- UID Light (LED UID) – Stato del LED UID quando è stata caricata la pagina. Oltre che mediante i pulsanti fisici disponibili sullo chassis del server, è possibile controllare lo stato della spia UID utilizzando il pulsante Turn UID On (Accendi UID).

  La spia UID consente di identificare e localizzare facilmente un sistema, in particolare negli ambienti rack ad elevata densità. La spia UID viene inoltre utilizzata per indicare che sul sistema host è in esecuzione un'operazione di importanza critica, ad esempio l'accesso alla console remota o l'aggiornamento del firmware.

  △ **ATTENZIONE:** Non scollegare mai l'alimentazione di un server mentre la spia UID sta lampeggiando.

  Lo stato corrente (ON o OFF) della spia UID è l'ultimo stato selezionato utilizzando uno di questi metodi. Se viene selezionato un nuovo stato mentre la spia UID sta lampeggiando, tale stato diventa quello corrente e risulta effettivo dal momento in cui la spia smette di lampeggiare. Quando la spia UID lampeggia, il relativo stato corrente viene visualizzato insieme a un tag, anch'esso lampeggiante. Quando la spia UID smette di lampeggiare, il tag viene rimosso.

  La spia UID non è supportata nei sistemi HP ProLiant ML310 G3.
- Last Used Remote Console (Ultima console remota utilizzata) – Ultima console remota avviata e relativa disponibilità. Questa opzione consente all'utente di avviare rapidamente la console remota

preferita. È possibile utilizzare la console remota se quest'ultima è disponibile e si dispone del privilegio utente appropriato. È possibile scegliere un'altra console utilizzando il collegamento Last Used Remote Console (Ultima console remota utilizzata).

- Latest IML Entry (Ultima voce IML) – La voce più recente inserita nel registro IML.
- iLO 2 Name (Nome iLO 2) - Nome assegnato al sottosistema iLO 2. Per impostazione predefinita, tale voce corrisponde alla parola iLO aggiunta al numero di serie del sistema. Questo valore viene utilizzato per il nome di rete e deve essere univoco.
- License Type (Tipo di licenza) - Indica se nel sistema è installata una funzionalità per cui è richiesta la licenza. Fornisce inoltre un collegamento a Administration>Licensing (Amministrazione>Gestione licenze). Alcune funzionalità di iLO 2 possono essere utilizzate solo se si dispone della relativa licenza.
- iLO 2 Firmware Version (Versione firmware iLO 2) – Informazioni relative alla versione del firmware di iLO 2 attualmente installata. Fornisce inoltre un collegamento alla pagina iLO 2 Release Notes (Note sulla versione di iLO 2) nella quale sono descritte le nuove funzionalità incluse nella versione corrente del firmware e in determinate versioni precedenti.
- IP Address (Indirizzo IP) - Indirizzo IP di rete del sottosistema iLO 2. Fornisce inoltre un collegamento a Administration>Network Settings (Amministrazione>Impostazioni di rete).
- Active Sessions (Sessioni attive) - Visualizza tutti gli utenti attualmente collegati a iLO 2.
- Latest iLO 2 Event Log Entry (Ultima voce del registro eventi di iLO 2) - Indica la voce più recente inserita nel registro eventi di iLO 2.
- iLO 2 Date (Data iLO 2) – La data, in formato MM/GG/AAAA, indicata dal calendario interno del sottosistema iLO 2. Il calendario interno di iLO 2 è sincronizzato con il sistema host al momento del POST e con Insight Agents in esecuzione.
- iLO 2Date/Time (Ora iLO 2) - Orologio interno del sottosistema iLO 2. L'orologio interno di iLO 2 è sincronizzato con il sistema host al momento del POST e con Insight Agents in esecuzione.

Riepilogo delle informazioni di sistema

Nella scheda System Information (Informazioni sul sistema) è riportato lo stato del sistema monitorato. Molte delle funzioni necessarie per il funzionamento e la gestione dei componenti del server HP ProLiant sono state spostate dal driver di sicurezza al microprocessore iLO 2. In questo modo tali funzioni risultano disponibili senza dovere installare e caricare il driver di sicurezza per il sistema operativo installato. Il microprocessore iLO 2 controlla questi dispositivi quando il server viene acceso durante l'avvio del server, l'inizializzazione del sistema operativo e il funzionamento. Il monitoraggio persiste fino al verificarsi di un guasto imprevisto del sistema operativo. Per accedere a System Information (Informazioni di sistema), fare clic su **System Status>System Information** (Stato del sistema>Informazioni di sistema). Viene visualizzata la scheda System Health Summary (Riepilogo sulla sicurezza del sistema). In System Information (Informazioni di sistema) vengono inoltre visualizzate le seguenti schede integrate sulla sicurezza: Fans (Ventole) (Ventole a pagina 81), Temperatures (Temperature) (Temperature a pagina 82), Power (Alimentazione) (Accensione a pagina 82), Processors (Processori) (Processori a pagina 82), Memory (Memoria) (Memoria a pagina 83) e NIC (Controller di rete) (NIC a pagina 83).

Nella scheda Summary (Riepilogo) è riportata una panoramica dello stato dei sottosistemi della piattaforma host monitorati, tra cui lo stato generale e il livello di ridondanza (capacità di gestire un guasto). I sottosistemi possono includere ventole, sensori di temperatura, alimentatori e moduli VRM.

- Fans (Ventole) – Stato delle ventole sostituibili nello chassis del server. Le informazioni includono l'area raffreddata da ciascuna ventola e la velocità corrente delle ventole.
- Temperatures (Temperature) – Condizioni di temperatura monitorate da sensori in varie ubicazioni dello chassis del server, nonché la temperatura del processore. La temperatura viene continuamente monitorata per assicurarsi che rimanga al di sotto della soglia di attenzione. Se viene superata la soglia di attenzione, la velocità delle ventole viene incrementata fino alla velocità massima consentita.
- VRMs (VRM) – Stato dei moduli VRM. Per ogni processore nel sistema deve essere presente un modulo VRM, la cui funzione è regolare l'alimentazione in modo da soddisfare i requisiti del relativo processore. Un modulo VRM guasto potrebbe compromettere l'alimentazione del processore e deve pertanto essere sostituito.
- Power Supplies (Alimentatori) – Visualizza la presenza e la condizione degli alimentatori installati.
  - OK – Indica che l'alimentatore è installato e funzionante.
  - Unpowered (Non acceso) – Indica che l'alimentatore è installato, ma non funzionante. Verificare che il cavo di alimentazione dia collegato.
  - Not present (Non presente) – Indica che l'alimentatore non è installato. In questo caso l'alimentazione non è ridondante.
  - Failed (Guasto) – Indica che l'alimentatore deve essere sostituito.

Per accedere alla pagina Summary (Riepilogo) da altre aree dell'interfaccia di iLO 2, fare clic su **System Status>System Information>Summary** (Stato del sistema>Informazioni di sistema>Riepilogo).

Ventole

iLO 2, insieme ad altri componenti hardware aggiuntivi, controlla il funzionamento e la velocità delle ventole. Le ventole forniscono il raffreddamento dei componenti necessario a garantire l'affidabilità e il funzionamento corretto. La disposizione, il design e la velocità delle ventole sono determinati in base alle temperature monitorate in diversi punti all'interno del sistema in modo da fornire il raffreddamento appropriato e allo stesso tempo garantire livelli minimi di rumore.

I criteri di funzionamento delle ventole possono differire da server a server a seconda della configurazione delle ventole e delle esigenze di raffreddamento. Le ventole vengono controllate in base alle temperature interne del sistema, aumentandone la velocità se è necessario un maggiore raffreddamento e rallentandole se il livello di raffreddamento è sufficiente. Nella remota eventualità di guasto di una ventola, a seconda dei criteri addottati, verrà aumentata la velocità delle altre ventole, l'evento verrà salvato nel registro IML e determinati indicatori LED si accenderanno.

Il monitoraggio dei sottosistemi delle ventole include diverse configurazioni, ossia raffreddamento sufficiente, ridondante e non ridondante. Sebbene il guasto di una ventola sia un evento raro, per garantire affidabilità e funzionamento continuo, la configurazione delle ventole nei server ProLiant è ridondante. Nei server ProLiant che supportano configurazioni ridondanti, il raffreddamento risulta sufficiente a garantire il funzionamento continuo anche nel caso di guasto di una o più ventole. In caso di guasto di una ventola, interventi di manutenzione o altri eventi che potrebbero compromettere il raffreddamento del server, infatti, iLO 2 aumenta la velocità delle ventole in modo da garantire un corretto funzionamento del server.

In configurazioni non ridondanti, o anche in configurazioni ridondanti se si guastano più ventole, è possibile che il sistema non riesca a fornire il raffreddamento necessario a proteggere il sistema da

eventuali danni e a garantire l'integrità dei dati. In tal caso, oltre ad applicare i criteri di gestione del raffreddamento, è possibile che il sistema operativo e il server vengano arrestati in modo controllato.

Nella scheda Fans (Ventole) è riportato lo stato delle ventole sostituibili presenti nello chassis del server. Le informazioni includono l'area raffreddata da ciascuna ventola e la velocità corrente delle ventole.

Temperature

Nella scheda Temperatures (Temperature) sono indicati la disposizione, lo stato, la temperature e le impostazioni di soglia dei sensori di temperatura presenti nello chassis del server. La temperatura viene continuamente monitorata per assicurarsi che rimanga al di sotto della soglia di attenzione. Se uno o più sensori rilevano una temperatura superiore alla soglia, iLO 2 esegue le azioni di recupero necessarie a impedire eventuali danni dei componenti del server.

- Se viene superata la soglia di attenzione, la velocità delle ventole viene incrementata fino alla velocità massima consentita.
- Se la temperatura supera il valore critico, viene avviato un arresto del server controllato.
- Se viene superata la soglia di pericolo, il server viene immediatamente spento per evitare danni permanenti.

I criteri di monitoraggio variano in base ai requisiti del server. Questi criteri in genere includono l'aumento della velocità delle ventole fino a ottenere il massimo raffreddamento, il salvataggio dell'evento di superamento della temperatura nel registro IML, segnalazioni visive dell'evento mediante indicatori LED e l'avvio di un arresto controllato del sistema operativo per evitare eventuali danni dei dati.

Una volta ripristinate le condizioni di temperatura, vengono adottati criteri aggiuntivi, quali il rallentamento delle ventole fino a tornare alla velocità normale, il salvataggio dell'evento nel registro IML, lo spegnimento degli indicatori LED e, se necessario, l'interruzione del processo di arresto.

Accensione

Nella scheda VRMs/Power Supplies (Moduli VRM/Alimentatori) è indicato lo stato di ogni modulo VRM e alimentatore. Per ogni processore nel sistema deve essere presente un modulo VRM, la cui funzione è regolare l'alimentazione in modo da soddisfare i requisiti del relativo processore. Un modulo VRM deve essere sostituito in caso di guasto, in quanto potrebbe compromettere l'alimentazione del processore.

iLO 2 monitora inoltre gli alimentatori nel sistema per garantire la massima disponibilità del server e del sistema operativo. I problemi degli alimentatori includono sottotensioni e altre condizioni elettriche, nonché lo scollegamento accidentale del cavo di alimentazione. Queste condizioni compromettono la ridondanza, in presenza di alimentatori ridondanti, o il funzionamento, in assenza di alimentatori ridondanti. In caso di guasto hardware di un alimentatore o di scollegamento del cavo di alimentazione, vengono inoltre salvati gli eventi appropriati nel registro IML e accesi gli indicatori LED relativi.

Mediante il monitoraggio iLO 2 consente anche di verificare che gli alimentatori siano installati correttamente. Queste informazioni sono visualizzate nella pagina System Information (Informazioni sul sistema). Esaminare le informazioni contenute in questa pagina e nel registro IML per determinare se occorre riparare o sostituire un alimentatore al fine di evitare interruzioni delle attività.

Processori

Nella scheda Processors (Processori) sono indicati gli alloggiamenti dei processori disponibili, il tipo di processore installato in ciascun alloggiamenti e un breve riepilogo delle condizioni del sottosistema del processore. Se tali informazioni sono disponibili, sono anche riportate la velocità del processore installato in MHz e la dimensione della cache.

Memoria

Nella scheda Memory (Memoria) vengono riportati gli alloggiamenti di memoria disponibili e l'eventuale tipo di memoria installato nell'alloggiamento.

NIC

Nella scheda NIC (Controller di rete) vengono visualizzati gli indirizzi MAC dei controller dell'interfaccia di rete integrati. In questa scheda non vengono visualizzati adattatori di rete aggiuntivi.

Registro di iLO 2

Nella pagina iLO 2 Log (Registro di iLO 2) viene visualizzato il registro eventi di iLO 2, in cui sono riportati gli eventi significativi rilevati da iLO 2. Sono inclusi eventi importanti del server, quali l'interruzione dell'alimentazione o il ripristino. Sono inoltre registrati eventi di iLO 2, quali i tentativi di accesso non autorizzato. Altri eventi registrati sono gli accessi tramite browser o console remota riusciti o non riusciti, qualsiasi evento di accensione virtuale o di riavvio e ogni azione di cancellazione del registro eventi. Vengono inoltre registrate alcune modifiche di configurazione, ad esempio la creazione o l'eliminazione di un utente.

iLO 2 consente la codifica della password per il rilevamento di tutti i tentativi di accesso e la registrazione di tutti gli accessi non riusciti. Authentication Failure Logging (Registrazione errori di autenticazione) consente di configurare i criteri di registrazione per le autenticazioni non riuscite. È possibile configurare il rilevamento dei tentativi di accesso non riusciti per ogni tentativo o per ogni secondo, terzo o quinto tentativo e acquisire il nome del client per ciascuna voce registrata in modo da migliorare le funzionalità di controllo negli ambienti DHCP, nonché per registrare il nome account, il nome del computer e l'indirizzo IP. Dopo un accesso non riuscito, iLO 2 genera degli allarmi e li invia a una console di gestione remota.

Gli eventi registrati da versioni successive del firmware di iLO 2 possono non essere supportati da versioni precedenti. Un evento registrato da un firmware non supportato verrà riportato come `UNKNOWN EVENT TYPE` (Tipo di evento sconosciuto). Per eliminare queste voci è possibile cancellare le informazioni presenti nel registro eventi o aggiornare il firmware alla versione supportata più recente.

Per accedere al registro di iLO 2, fare clic su **System Status>iLO 2 Log** (Stato del sistema>Registro di iLO 2).

Per cancellare le informazioni presenti nel registro eventi:

1. Fare clic su **Clear Event Log** (Cancellazione registro eventi) per cancellare tutte le informazioni registrate in precedenza.
2. Fare clic su **OK** per confermare l'operazione di cancellazione del registro degli eventi. Viene registrata una riga per indicare che l'azione è stata eseguita.

IML

Nella pagina IML (Registro di gestione integrato) viene visualizzato il registro di gestione integrato (IML, Integrated Management Log), un registro di eventi significativi verificatisi nel server secondo quanto riportato dai diversi componenti software. Gli eventi sono generati dalla ROM del sistema e da servizi quali il driver di sicurezza di gestione del sistema. Il registro di gestione integrato permette di visualizzare gli eventi del server remoto registrati. Sono inclusi tutti gli eventi specifici del server registrati dal driver di sicurezza del sistema, incluse le informazioni relative al sistema operativo e i codici POST basati sulla ROM. Per ulteriori informazioni, consultare la documentazione del server.

Le voci presenti nel registro di gestione integrato offrono informazioni significative durante la diagnosi dei problemi e consentono di prevedere possibili problemi prima che questi si verifichino. Si consiglia di effettuare azioni preventive per evitare possibili interruzioni delle attività. iLO 2 aggiorna il registro di

gestione integrato, a cui è possibile accedere utilizzando un browser supportato, anche quando il server è spento. La possibilità di visualizzare il registro eventi anche quando il server è spento può risultare utile per la risoluzione dei problemi del server host remoto.

È possibile ordinare il registro facendo clic sull'intestazione di una qualsiasi colonna di dati. Una volta completato l'ordinamento, se si fa di nuovo clic sulla stessa intestazione di colonna, l'ordinamento corrente viene invertito. L'ordinamento e la visualizzazione di registri di notevoli dimensioni possono richiedere diversi minuti. È possibile cancellare gli eventi presenti nel registro utilizzando la home page degli agenti Web di Insight Manager in esecuzione sul server.

Il processore iLO 2 inserisce nel registro di gestione integrato, in base al numero di occorrenze nel sistema, gli eventi indicati di seguito:

- Fan inserted (Inserimento ventola)
- Fan removed (Rimozione ventola)
- Fan failure (Guasto ventola)
- Fan degraded (Danneggiamento ventola)
- Fan repaired (Riparazione ventola)
- Fan redundancy lost (Perdita ridondanza ventole)
- Fans redundant (Ventole ridondanti)
- Power supply inserted (Inserimento alimentatore)
- Power supply removed (Rimozione alimentatore)
- Power supply failure (Guasto alimentatore)
- Power supplies redundancy lost (Perdita ridondanza alimentatori)
- Power supplies redundant (Alimentatori ridondanti)
- Temperature over threshold (Temperatura superiore alla soglia massima)
- Temperature normal (Temperatura normale)
- Automatic shutdown started (Avvio spegnimento automatico)
- Automatic shutdown cancelled (Annullamento spegnimento automatico)

Diagnostica

L'opzione Diagnostics (Diagnostica) nella scheda System Status (Stato del sistema) consente di visualizzare la schermata Server and iLO 2 Diagnostics (Diagnostica del server e di iLO 2). Nella schermata Server and iLO 2 Diagnostic (Diagnostica del server e di iLO 2) sono visualizzati i risultati del test automatico di iLO 2 e vengono fornite opzioni per generare un NMI nel sistema e reimpostare iLO 2.

NOTA: Il server di directory non è disponibile quando è collegato tramite la porta di diagnostica. È possibile accedere solo utilizzando un account locale.

La pagina Diagnostics (Diagnostica) contiene le seguenti sezioni:

- Non-Maskable Interrupt (NMI)

  La sezione Non-Maskable Interrupt (Interrupt non mascherabile) contiene il pulsante Generate NMI to System (Genera NMI nel sistema) che consente di arrestare il sistema operativo per scopi di debug. Si tratta di una funzione avanzata da utilizzare esclusivamente per il debug a livello del

kernel. Gli utilizzi possibili della funzionalità Generate NMI to System (Genera NMI nel sistema) comprendono quanto riportato di seguito:

- Utilizzo della funzionalità Demonstrate ASR (Dimostrazione ASR) soltanto se il driver di sicurezza di gestione del sistema è presente e se ASR è abilitato. Riavvio automatico del sistema host dopo il verificarsi di un NMI.
- Utilizzo della funzionalità di debug nel caso in cui un'applicazione software determini il blocco del sistema. Il pulsante Generate NMI to System (Genera NMI nel sistema) consente di eseguire il debugger del sistema operativo.
- Avvio del dump di un host senza risposta nel caso in cui si desideri acquisire il contesto del server.

  Per generare un NMI è necessario disporre del privilegio Virtual Power and Reset (Accensione virtuale e reimpostazione). Un NMI non previsto segnala in genere un errore irreversibile nella piattaforma host. Quando il sistema operativo dell'host riceve un NMI imprevisto, viene visualizzata una schermata blu, viene generato un messaggio di tipo Panic, si verifica un arresto anomalo del sistema o un errore irreversibile, anche se il sistema operativo non risponde o è bloccato. La generazione di un NMI imprevisto può essere utilizzata anche per la diagnosi di uno stato di blocco critico del sistema operativo. La generazione di un NMI imprevisto determina il crash del sistema operativo, con conseguente interruzione del servizio e perdita di dati.

  La generazione di un NMI imprevisto dovrebbe essere utilizzata soltanto per scopi di diagnostica in casi estremi, ad esempio quando il sistema operativo non funziona correttamente e l'esecuzione di tale operazione è stata consigliata da un'organizzazione di supporto dotata delle competenze necessarie. La generazione di un NMI imprevisto come strumento di diagnostica e debug viene utilizzata principalmente quando il sistema operativo non è più disponibile. La generazione di un NMI imprevisto non deve essere eseguita durante il normale funzionamento del server. Il pulsante Generate NMI to System (Genera NMI nel sistema) non esegue il normale arresto del sistema operativo.

- iLO 2 Self-Test Results

  Nella sezione iLO 2 Self-Test Results (Risultati del test automatico di iLO 2) vengono visualizzati i risultati della diagnostica interna di iLO 2. iLO 2 esegue una serie di procedure di inizializzazione e diagnostica nei sottosistemi del sistema iLO 2. I risultati sono visualizzati nella schermata Server and iLO 2 Diagnostics (Diagnostica server e iLO 2). In condizioni normali, per tutti i sottosistemi sottoposti a test viene visualizzato il messaggio Passed (Superato). Per ciascun test viene visualizzato uno dei seguenti risultati: Passed (Superato), Fault (Non superato), N/A (N/D)

  Lo stato dei test automatici è indicato dai relativi risultati e consente di identificare le aree problematiche. Se lo stato del test è Fault (Non superato), seguire le istruzioni visualizzate sullo schermo. I test specifici che vengono eseguiti dipendono dal sistema in uso. Non tutti i test vengono eseguiti su tutti i sistemi. Per stabilire quali test vengono eseguiti automaticamente sul sistema utilizzato, vedere la pagina iLO 2 Diagnostics (Diagnostica iOL 2).

- Reset Integrated Lights-Out 2

  La sezione Reset Integrated Lights-Out 2 (Reimposta Integrated Lights-Out 2) contiene il pulsante Reset (Reimposta) che consente di riavviare il processore iLO 2. L'utilizzo di questo pulsante non determina alcuna modifica di configurazione. Se si utilizza il pulsante Reset (Reimposta), tutte le connessioni attive a iLO 2 vengono interrotte e gli eventuali aggiornamenti del firmware in corso vengono completati. Per reimpostare iLO 2 utilizzando questa opzione è necessario disporre del privilegio Configure iLO 2 (Configura iLO 2).

Insight Agents

HP Insight Management Agents supporta un'interfaccia del browser che consente di accedere ai dati di gestione runtime tramite la home page di HP System Management. La home page di HP System Management è un'interfaccia sicura basata su Web che consente di consolidare e semplificare la gestione dei singoli server e sistemi operativi. Grazie all'aggregazione dei dati di HP Insight Management Agents e di atri strumenti di gestione, la home page di System Management fornisce un'interfaccia intuitiva che consente di esaminare nel dettaglio i dati relativi allo stato e alla configurazione, misurare il livello di prestazioni, stabilire i valori soglia del sistema e visualizzare informazioni di controllo sulla versione del software.

Gli agenti possono fornire automaticamente il collegamento a iLO 2. In alternativa, è possibile immettere manualmente tale collegamento utilizzando Administration/Management (Amministrazione/Gestione).

Per ulteriori informazioni, vedere "Integrazione di HP Systems Insight Manager" e visitare il sito Web HP all'indirizzo http://www.hp.com/servers/manage.

Console remota di iLO 2

La console remota di iLO 2 reindirizza la console del server host al browser del client di rete, consentendo un completo accesso in modalità testo (standard) e grafica, tramite tastiera e mouse, al server host remoto (se si dispone di un'apposita licenza). iLO 2 utilizza la tecnologia virtuale KVM per migliorare le prestazioni della console remota rispetto ad altre soluzioni KVM equiparabili.

La console remota consente di osservare i messaggi di avvio del POST al riavvio del server host remoto e di eseguire le routine basate sulla ROM per la configurazione dell'hardware del server host remoto. Quando si installano sistemi operativi in remoto, la console grafica remota consente di visualizzare e controllare lo schermo del server host durante l'intero processo di installazione.

La console remota consente il controllo completo su un server host remoto, consentendo inoltre l'accesso al file system remoto e alle unità di rete. Consente inoltre di modificare le impostazioni hardware e software del server host remoto, installare applicazioni e driver, cambiare la risoluzione video del server remoto ed eseguire il normale arresto del sistema remoto.

A iLO 2 possono accedere contemporaneamente 10 utenti. A una console remota integrata condivisa possono invece accedere contemporaneamente soltanto quattro utenti. Se si tenta di aprire la console remota mentre è già in uso, viene visualizzato un messaggio di avviso che segnala l'uso della console da parte di un altro utente. Per informazioni su come visualizzare la sessione della console remota attualmente in corso, vedere la sezione "Console remota condivisa" (Console remota condivisa a pagina 97). Per acquisire il controllo della sessione, utilizzare la funzionalità Remote Console Acquire (Acquisizione console remota). Per ulteriori informazioni, vedere la sezione "Acquisizione della console remota" (Acquisizione della console remota a pagina 100).

Nella pagina Remote Console Information (Informazioni sulla console remota) sono inclusi collegamenti alle diverse opzioni di accesso alla console remota. Dopo aver deciso quale opzione utilizzare, fare clic sul collegamento appropriato. iLO 2 fornisce le seguenti opzioni di accesso alla console remota:

- Integrated Remote Console (Console remota integrata) (Console remota integrata a pagina 92) - Consente di accedere alle opzioni KVM del sistema e gestire l'accensione e i supporti virtuali da un'unica console in Microsoft® Internet Explorer.
- Integrated Remote Console Fullscreen (Console remota integrata a schermo intero) (Console remota integrata a schermo intero a pagina 92) – Ridimensiona la finestra della console remota integrata impostandola sulla stessa risoluzione dello schermo dell'host remoto.

  Le opzioni Integrated Remote Console (Console remota integrata) e Integrated Remote Console Fullscreen (Console remota integrata a schermo intero) utilizzano ActiveX e richiedono Microsoft® Internet Explorer™.

- Remote Console (Console remota) (Console remota a pagina 101) - Fornisce l'accesso alle opzioni KVM del sistema mediante una console basata su applet Java. La console remota è una versione rielaborata della tradizionale console del prodotto originale iLO. Per poter utilizzare la console remota è necessario che nel sistema client sia installato Java™. La console remota funziona con tutti i sistemi operativi e i browser supportati da iLO 2.
- Remote Serial Console (Console seriale remota) (Console seriale remota a pagina 108) - Fornisce l'accesso a una console seriale VT320 mediante una console basata su applet Java collegata alla porta seriale virtuale di iLO 2. La console seriale remota è disponibile senza licenza aggiuntiva e può essere utilizzata con i sistemi operativi host per cui non è necessario l'accesso alla console grafica.

La versione standard di iLO 2 consente l'accesso alla console dall'accensione del server al POST. La console remota integrata, la console remota integrata a schermo intero e la console remota sono console grafiche remote in grado di trasformare il browser supportato in un vero e proprio desktop virtuale, garantendo all'utente il pieno controllo di mouse, tastiera e schermo del server host. La console indipendente dal sistema operativo supporta le modalità grafiche per visualizzare le attività del server host remoto, quali le operazioni di arresto e di avvio (se si dispone dell'apposita licenza).

L'accesso dalla console remota al server host dopo il POST del server è una funzionalità che richiede un'apposita licenza e può essere acquistata insieme a licenze opzionali. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20). Per accedere alla console remota di iLO 2, fare clic su **Remote Console** (Console remota). Viene visualizzata la pagina Remote Console Information (Informazioni sulla console remota).

Panoramica sulla console remota e opzioni di licenza

Per visualizzare le connessioni della console remota e della console remota integrata è necessario utilizzare un programma client in grado di elaborare i comandi grafici di iLO 2. Per la visualizzazione dei dati grafici di iLO 2 vengono forniti due client:

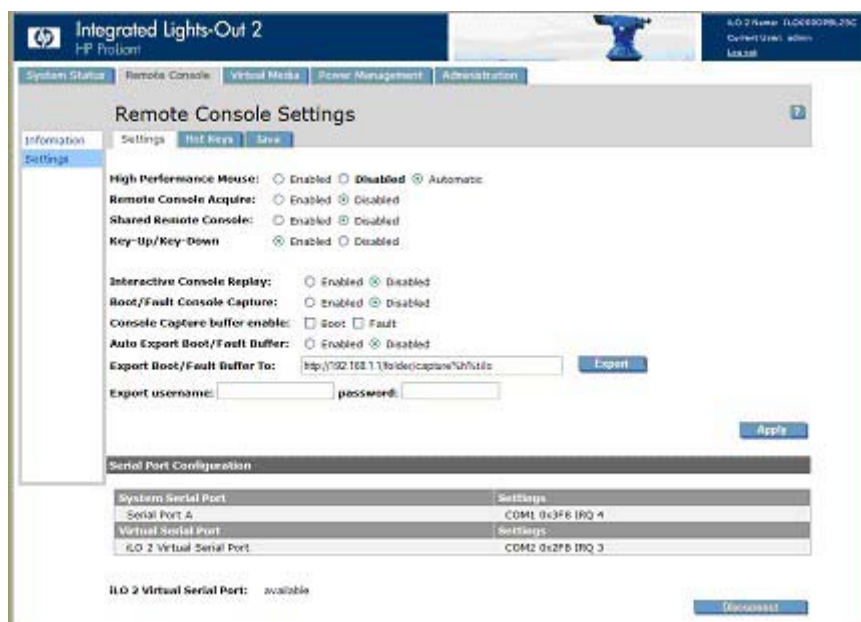
- Console remota basata su Java™
- Console remota integrata basata su Active X di Windows®

Per i client che non sono in grado di interpretare i comandi grafici di iLO 2, ad esempio SSH e telnet, è necessario utilizzare la console seriale remota di iLO 2 o acquistare una licenza iLO Advanced per utilizzare la console di testo dopo il POST.

Le console ESX, in particolare la console ESX 1, non supportano pienamente la console remota e la console remota integrata di iLO 2. ESX non supporta la console seriale remota.

I blade iLO 2 vengono forniti con iLO 2 Standard Blade Edition, che include la console remota. I modelli HP ProLiant ML e HP ProLiant DL invece vengono forniti con la licenza iLO Standard, che non include la console remota o la console remota integrata. Una volta iniziato l'avvio del sistema operativo, infatti, sui modelli HP ProLiant ML e ProLiant DL viene visualizzato un messaggio che richiede la licenza iLO 2 Advanced. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20).

Impostazioni della console remota

Le impostazioni e le opzioni relative alla console remota di iLO 2 vengono configurate nella pagina Remote Console Settings (Impostazioni della console remota). Per accedere alla pagina Remote Console Settings (Impostazioni della console remota), fare clic su **Remote Console>Settings** (Console remota>Impostazioni).

La pagina Remote Console Settings (Impostazioni della console remota) include tre schede:

Settings (Impostazioni)

- Le impostazioni High Performance Mouse (Mouse ad alte prestazioni) consentono di ridurre i problemi relativi alla sincronizzazione del mouse della console remota. Questa funzionalità non è tuttavia supportata in tutti i sistemi operativi. Le modifiche alle impostazioni vengono rese effettive quando la console remota viene avviata o riavviata. Sono disponibili le opzioni riportate di seguito:
  - Disabled (Disabilitato) – Consente al mouse di utilizzare la modalità a coordinate relative, compatibile con la maggior parte dei sistemi operativi.
  - Enabled (Abilitato) – Consente al mouse di utilizzare la modalità a coordinate assolute, eliminando così i problemi di sincronizzazione nei sistemi operativi supportati.
  - Automatic (Automatico) – Consente a iLO 2 di selezionare la modalità mouse appropriata quando il driver di iLO 2 viene caricato nel sistema operativo host. La modalità selezionata viene mantenuta fino a quando non viene specificata una modalità differente nel momento in cui viene caricato il driver del sistema operativo o si sceglie un'altra impostazione.
- L'opzione Remote Console Acquire (Acquisizione console remota) consente a un utente di acquisire la sessione della console remota da un altro utente. Questa impostazione abilita o disabilita la funzionalità di acquisizione.
- L'opzione Shared Remote Console (Console remota condivisa) consente a più utenti contemporaneamente di visualizzare e controllare la console del server. Questa impostazione abilita o disabilita la funzionalità di condivisione.
- L'opzione Interactive Console Replay (Riproduzione console interattiva) consente di riprodurre le immagini acquisite relative alle operazioni di avvio e ai tentativi non riusciti, nonché le immagini della console acquisite manualmente dall'utente.
- L'opzione Key-Up/Key-Down (Tastiera attivata/disattivata) consente di attivare/disattivare l'utilizzo del modello di tastiera HID report o del modello di tastiera a codici ASCII ed ESC nella console remota integrata. Il modello di tastiera HID report è attivato per impostazione predefinita, ma può causare caratteri ripetitivi nel caso di reti a latenza elevata. Se si riscontrano caratteri ripetuti quando si utilizza la console remota integrata, impostare Key-Up/Key-Down (Tastiera attivata/disattivata) su **Disabled** (Disabilitato).

- L'opzione Boot/Fault Console Capture (Acquisizione sequenze di avvio/errore della console) consente di acquisire video della console nei buffer interni relativi alle sequenze di avvio e di errore. Lo spazio dei buffer interni è limitato all'acquisizione della sequenza di avvio o di errore più recente. Lo spazio buffer è limitato. Quanto più è dinamica e superiore la risoluzione grafica della console del server, minore è la quantità di dati che è possibile memorizzare nel buffer. Selezionare il tipo di video da acquisire utilizzando le seguenti opzioni:
  - L'opzione Console Capture buffer enable (Abilita buffer acquisizione console) consente di selezionare il tipo di sequenza di console da acquisire. È possibile attivare uno dei buffer o entrambi i buffer contemporaneamente. Poiché i buffer condividono la stessa area di dati interna, l'attivazione di entrambi riduce la quantità di video della console che è possibile acquisire. Per ottimizzare l'utilizzo dei buffer, è possibile modificare i buffer attivati in qualsiasi momento. Quando la configurazione dei buffer viene modificata, entrambi i buffer vengono reimpostati e le informazioni in essi contenute vanno perse.
  - L'opzione Auto Export/Fault Buffer (Esportazione automatica/Buffer errori) consente di abilitare o disabilitare l'esportazione automatica dei dati della console acquisiti.
- L'opzione Export Boot/Fault Buffer (Esporta buffer di avvio/errori) consente di specificare il percorso URL di un server Web che accetta un trasferimento di dati mediante PUT o POST. Ad esempio: `http://192.168.1.1/images/capture%h%t.iLO` trasferisce i buffer di acquisizione interni in un server Web all'indirizzo IP 192.168.1.1 e memorizza i dati nella cartella `images` utilizzando il nome file `captureServerNameDateTime-Boot(o Fault).iLO`, dove:
  - %h specifica l'aggiunta del nome del server al nome file.
  - %t specifica che nel nome file verrà incluso un timestamp.
  - Boot o Fault viene aggiunto automaticamente per denotare il tipo di buffer, ovvero un buffer per le sequenze di avvio o per le sequenze di errore.

    Per ulteriori informazioni sulla configurazione del server Web e sulla modalità di configurazione di un server Web Apache per accettare i buffer di acquisizione esportati, vedere la sezione "Configurazione di Apache per i buffer di acquisizione esportati" (Configurazione di Apache per i buffer di acquisizione esportati a pagina 220).
  - Il pulsante Export (Esporta) consente di eseguire un'esportazione manualmente.
  - Il campo Export username (Nome utente esportazione)visualizza il nome utente del server Web specificato nell'URL.
  - Il campo Password visualizza la password del server Web specificata nell'URL.

    Dopo avere apportato le modifiche, fare clic su **Apply** (Applica).
- Nella sezione Serial Port Configuration (Configurazione porta seriale) sono visualizzate le impostazioni correnti delle porte seriali del sistema e della porta seriale virtuale. Vengono inoltre visualizzate le impostazioni del sistema e delle porte seriali virtuali, con l'indicazione delle porte COM in uso e dei numeri IRQ.
- iLO 2 Virtual Serial Port (Porta seriale virtuale di iLO 2) visualizza lo stato corrente della connessione alla porta seriale virtuale. Le modalità disponibili sono: In use (In uso) in modalità Raw o In use (In uso) in modalità Normale. Se la connessione è impostata su In use (In uso), è disponibile il pulsante Disconnect (Disconnetti) che può essere utilizzato per interrompere la connessione a una porta seriale virtuale. La modalità Raw indica che un client viene connesso mediante l'utility WiLODbg.exe, utilizzata per il debug del kernel Windows® in remoto.

Hot Keys (Tasti di scelta rapida) consente di definire le sequenze di tasti che verranno trasmesse al server host remoto in seguito alla pressione di un tasto di scelta rapida. I tasti di scelta rapida della console remota consentono di creare sequenze specifiche di tasti, quali Alt-Tab e Alt-SysRq da trasferire

al server dalla sessione Java™ della console remota. Per ulteriori informazioni, vedere la sezione "Tasti di scelta rapida della console remota" (Tasti di scelta rapida della console remota a pagina 90).

Java consente di visualizzare i requisiti Java™ per ciascun sistema operativo supportato e un collegamento per il download di Java™. Per ulteriori informazioni, vedere la sezione "Browser e sistemi operativi client supportati" (Browser e sistemi operativi client supportati a pagina 6).

Tasti di scelta rapida della console remota

Nella pagina Program Remote Console Hot Keys (Programmazione dei tasti di scelta rapida della console remota) è possibile definire fino a sei differenti combinazioni di tasti assegnate a ciascun tasto di scelta rapida. Quando si preme un tasto di scelta rapida nella console remota, sui sistemi client viene trasmessa al server host remoto la combinazione di tasti definita (tutti i tasti premuti contemporaneamente), anziché il tasto di scelta rapida. Per accedere ai simboli AltGr delle tastiere internazionali, definire tali simboli utilizzando i tasti di scelta rapida. Per un elenco dei tasti di scelta rapida supportati, vedere la sezione "Tasti di scelta rapida supportati" (Tasti di scelta rapida supportati a pagina 90).

Durante una sessione della console remota, i tasti di scelta rapida della console remota sono attivi tramite la console remota integrata, l'applet della console remota e, durante una sessione della console remota basata su testo, tramite un client Telnet. Quando si utilizza la console remota integrata, lo stato dei LED associati a BLOC NUM, BLOC MAIUSC e BLOC SCORR sulla tastiera client non riflette necessariamente lo stato della tastiera del server. La pressione di uno di questi tasti determina tuttavia la modifica dello stato di blocco sul server.

Per definire un tasto di scelta rapida della console remota:

1. Fare clic su **Remote Console>Hot Keys** (Console remota>Tasti di scelta rapida).
2. Selezionare il tasto di scelta rapida che si desidera definire. Nelle caselle a discesa, selezionare la sequenza di tasti da trasmettere al server host quando si preme il tasto di scelta rapida.
3. Dopo aver definito le sequenze di tasti, fare clic sul pulsante **Save Hot Keys** (Salva tasti di scelta rapida).

La schermata Program Remote Console Hot Keys (Programmazione dei tasti di scelta rapida della console remota) comprende anche l'opzione Reset Hot Keys (Reimposta tasti di scelta rapida), che consente di cancellare tutte le voci nei campi dei tasti di scelta rapida. Fare clic su **Save Hot Keys** (Salva tasti di scelta rapida) per salvare i campi cancellati.

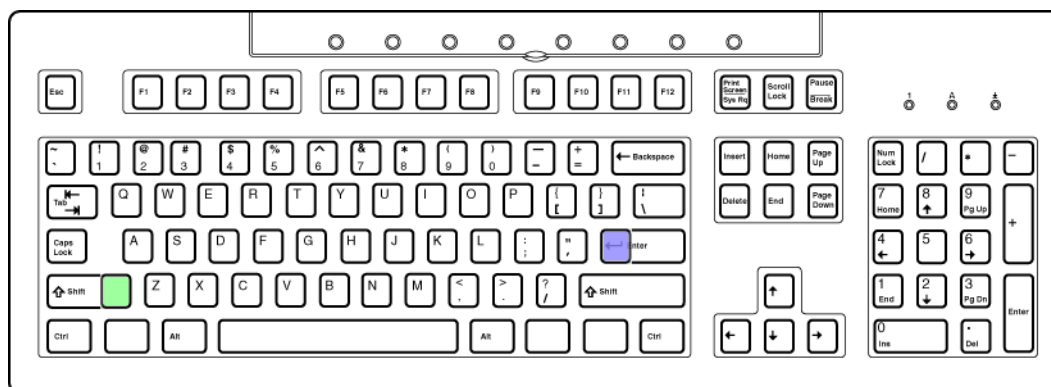
Tasti di scelta rapida supportati

La pagina di programmazione dei tasti di scelta rapida della console remota consente di definire fino a 6 differenti gruppi di tasti di scelta rapida da utilizzare durante una sessione della console remota. Ciascun tasto di scelta rapida può essere costituito da una combinazione di un massimo di cinque tasti che vengono inviati al computer host ogni volta che si preme il tasto di scelta rapida nel corso di una sessione della console remota. In tal caso viene trasmessa la combinazione di tasti selezionata (tutti i tasti premuti contemporaneamente) anziché i singoli tasti. Per ulteriori informazioni, vedere la sezione "Tasti di scelta rapida della console remota" (Tasti di scelta rapida della console remota a pagina 90). La seguente tabella riporta i tasti utilizzabili per combinare una sequenza di tasti di scelta rapida per la console remota.

ESC	F12	:	o
ALT-L	" " (Barra spaziatrice)	<	p
ALT-R	!	>	q
MAIUSC-L	#	=	r

MAIUSC-R	$	?	s
INS	%	@	t
CANC	&	[	u
HOME	~	]	v
FINE	(	\	w
PG SU	)	^	x
PG GIÙ	*	_	y
INVIO	+	a	z
TAB	-	b	{
BREAK	.	c	}
F1	/	d	|
F2	0	e	;
F3	1	f	'
F4	2	g	CTRL-L
F5	3	h	CTRL-R
F6	4	i	TASTNUM +
F7	5	j	TASTNUM -
F8	6	k	BLOC SCORR
F9	7	l	BACKSPACE
F10	8	m	R SIST
F11	9	n	

Tasti di scelta rapida e tastiere internazionali

Per impostare tasti di scelta rapida su una tastiera internazionale, selezionare su tale tastiera i tasti che si trovano nella stessa posizione in una tastiera statunitense. Per creare un tasto di scelta rapida utilizzando il tasto AltGr delle tastiere internazionali, utilizzare la combinazione ALT-R indicata nell'elenco di tasti riportato di seguito. Per selezionare i tasti, utilizzare lo schema della tastiera statunitense visualizzato di seguito.

Nella tastiera statunitense non sono presenti tasti colorati.

- Il tasto verde corrisponde al tasto \ nelle tastiere non statunitensi e al tasto | nella tastiera internazionale.
- Il tasto viola corrisponde al tasto # nelle tastiere non statunitensi e al tasto ~ nella tastiera internazionale.

Tasti di scelta rapida e porta seriale virtuale

Quando si stabilisce la connessione alla porta seriale virtuale di iLO 2 utilizzando Telnet, la sequenza di tasti CTRL+P+! (tasti CTRL, P, MAIUSC e 1 premuti contemporaneamente) causa in genere il riavvio del server remoto.

Per spegnere il server remoto utilizzare la sequenza di tasti CTRL+P 6, per accenderlo utilizzare la sequenza CTRL+P 1.

Se iLO 2 non risponde, chiudere la sessione della porta seriale virtuale. iLO 2 verrà riavviato automaticamente e sarà nuovamente funzionante entro circa tre minuti.

Console remota integrata a schermo intero

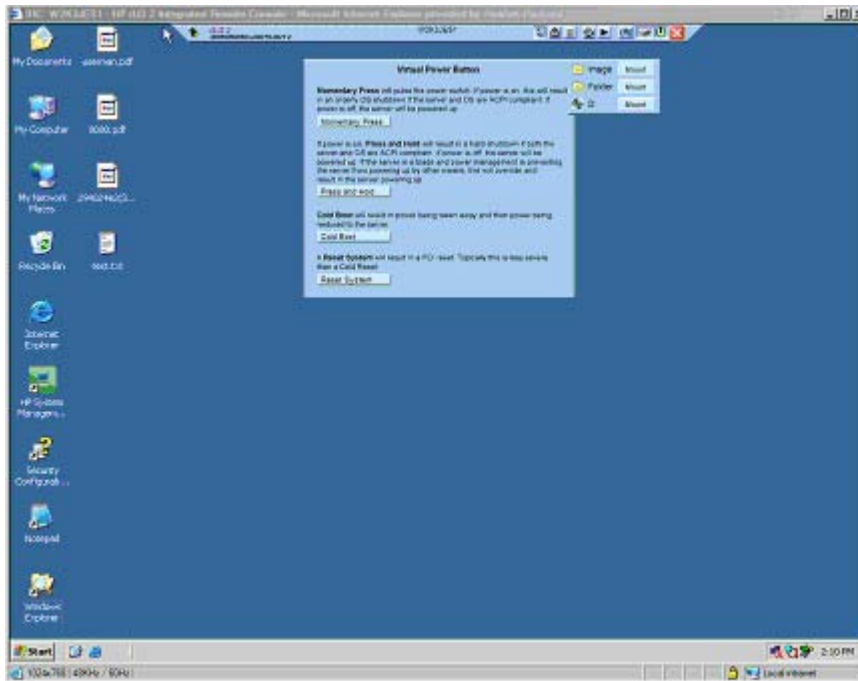
La console remota integrata a schermo intero consente di modificare le dimensioni della console in modo che venga visualizzata con la stessa risoluzione dello schermo dell'host remoto. Per tornare al desktop del client, chiudere la console.

La console remota integrata a schermo intero comporta il ridimensionamento del client in base alla stessa risoluzione del server remoto. La console remota integrata a schermo intero tenta di rilevare le impostazioni di visualizzazione del client ottimali per la risoluzione selezionata. Per alcuni monitor potrebbero tuttavia verificarsi dei problemi a causa della massima frequenza di aggiornamento supportata dall'adattatore video. In questo caso, verificare le proprietà del desktop. Fare clic con il pulsante destro del mouse su **Desktop**, selezionare **Proprietà>Impostazioni>Avanzate>Monitor** e selezionare una frequenza di aggiornamento più bassa.

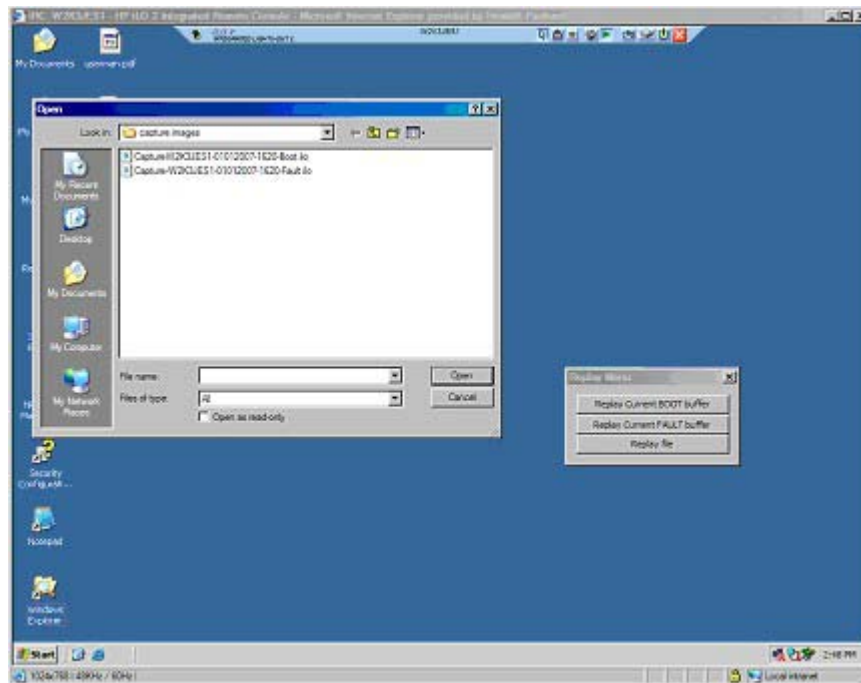
Per ulteriori informazioni sulla visualizzazione della console remota integrata a schermo intero, vedere la sezione "Console remota integrata" (Console remota integrata a pagina 92).

Console remota integrata

La console remota integrata offre un'interfaccia a elevate prestazioni per i client Windows® e combina le funzionalità KVM, l'accensione virtuale e i supporti virtuali. La funzionalità Integrated Remote Console (Console remota integrata) è un controllo ActiveX che viene eseguito da Microsoft® Internet Explorer. Questa funzionalità richiede un'apposita licenza e può essere acquistata insieme a licenze opzionali. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20).

Se attivata tramite la schermata Remote Console Settings (Impostazioni della console remota), SMASH CLI (OEM) o RIBCL, la console remota integrata supporta quattro sessioni di console remota simultanee con lo stesso server. Per ulteriori informazioni sull'utilizzo di più sessioni di console remota, vedere la sezione "Console remota condivisa" (Console remota condivisa a pagina 97).

Nella console remota integrata e nella console remota integrata a schermo intero sono disponibili una barra dei menu e una serie di pulsanti. Sulla barra dei menu sono disponibili le seguenti opzioni:

- Remote Console Replay (play icon) [Riproduzione console remota (icona Play)] – Visualizza la finestra di dialogo Replay Menu (Menu Riproduci), se è attivata l'acquisizione delle sequenze di avvio o di errore della console, o la finestra di dialogo Open File (Apri file), se l'acquisizione delle sequenze di avvio/errore della console non è attivata.
    - Replay Current BOOT buffer (Riproduci buffer BOOT corrente) e Replay Current FAULT buffer (Riproduci buffer FAULT corrente) – Consentono di trasferire al client i buffer acquisiti internamente utilizzando la porta Console Replay (Riproduzione console) specificata nella scheda Administration>Access (Amministrazione>Accesso). Per passare dal menu Remote Console (Console remota) al menu Replay Console (Console riproduzione), fare clic su **Replay Current BOOT buffer** (Riproduci buffer BOOT corrente) o **Replay Current FAULT buffer** (Riproduci buffer FAULT corrente).

- Replay file (Riproduci file) – Visualizza la finestra di dialogo Apri nella quale è possibile visualizzare un file precedentemente salvato. Quando si seleziona un file e si fa clic su **Open** (Apri), il menu Remote Console (Console remota) viene sostituito dal menu Replay Console (Console riproduzione).

- Replay (Riproduci) [icona Play nel menu principale] – Visualizza la console di riproduzione. La console di riproduzione consente di controllare la riproduzione dei buffer di dati selezionati e indica il tempo di riproduzione trascorso.

La console di riproduzione comprende le seguenti opzioni:

- Fare clic su **Play** (Riproduci) per avviare la riproduzione. Dopo aver fatto clic su Play (Riproduci) è possibile:

  — Fare clic su **Pause** (Pausa) per interrompere la riproduzione e mantenere la posizione corrente. Per riavviare la riproduzione, fare clic su **Play** (Riproduci) dallo stato di pausa. La riproduzione riprenderà dalla posizione corrente.

  — Fare clic su **Stop** (Interrompi) per interrompere la riproduzione e reimpostarla all'inizio del buffer di dati.

  — Fare clic su **Fast-forward** (Avanti veloce) per aumentare la velocità di riproduzione di 2, 4 o 8 volte la velocità normale.

- Al termine della riproduzione viene visualizzato il pulsante Close (Chiudi). Fare clic su **Close** (Chiudi) per chiudere la console di riproduzione e visualizzare la barra dei menu della console remota.

- Record (Registra) [icona macchina fotografica] – Consente di registrare manualmente il video della console del server corrente. Fare clic su **Record** (Registra) per visualizzare una finestra di dialogo in cui è possibile specificare il nome file e il percorso in cui salvare la sessione di registrazione corrente. Durante una sessione di registrazione, il pulsante Record (Registra) appare disattivato

e di colore verde. Quando è attivato, tutte le attività della console del server visualizzate nella console remota integrata vengono salvate nel file specificato. Se si fa clic su **Record** (Registra) durante una sessione di registrazione, la sessione viene interrotta e il pulsante Record (Registra) risulta nuovamente disattivato. Per riprodurre la registrazione, fare clic su **Replay** (Riproduci).

- Control (Controllo) – Consente al responsabile della sessione di riprendere il controllo completo nel caso in cui sia stato concesso il controllo a un client satellite.
- Lock (Blocco) – Consente di impedire la visualizzazione di ulteriori richieste di client satelliti nella console del responsabile della sessione.
- Client List (Elenco client) – Visualizza il nome utente e il nome DNS (se disponibile) o l'indirizzo IP dei client satelliti correnti.
- Drive (Unità) – Visualizza tutti i supporti disponibili.
- Power (Alimentazione) [icona di alimentazione verde] – Visualizza lo stato di alimentazione e consente di accedere alle opzioni di alimentazione. Il pulsante di alimentazione è di colore verde quando il server è acceso. Quando si fa clic su **Power** (Alimentazione) viene visualizzata la schermata Virtual Power Button (Pulsante accensione virtuale) contenente quattro opzioni: Momentary Press (Pressione momentanea), Press and Hold (Pressione mantenuta), Cold Boot (Avvio a freddo) e Reset System (Reimposta sistema).

  Quando i pulsanti Drives (Unità) o Power (Alimentazione) sono selezionati, il menu visualizzato rimane attivo anche se si sposta il mouse dalla barra dei menu.
- CAD – Consente di avviare una finestra di dialogo per l'invio dei tasti Ctrl-Alt-Canc (o uno dei sei tasti di scelta rapida) al server.
- Thumb tack (Puntina da disegno) – Consente di mantenere aperto il menu principale della console remota o di comprimerlo quando si allontana il mouse.
- Exit (Esci) [icona X rossa] – Consente di chiudere e uscire dalla console remota.

Le funzioni di protezione avanzate di Internet Explorer 7 prevedono la visualizzazione della barra degli indirizzi in tutte le finestre aperte di recente. Se si desidera rimuovere la barra degli indirizzi dalla console remota integrata, è necessario modificare l'impostazione Security (Protezione) dal livello predefinito. Per rimuovere la barra degli indirizzi, impostare "Consenti ai siti Web l'apertura di finestre senza indirizzo o barra di stato" su **Attiva**.

Ottimizzazione delle prestazioni del mouse per la console remota o la console remota integrata

Per garantire il funzionamento ottimale della console remota,in alcune configurazioni di Microsoft® Windows® è necessario impostare la velocità correttamente la velocità del mouse.

SLES 9

Determinare il tipo di mouse impostato nella console remota utilizzando il comando `xsetpointer -l` per visualizzare l'elenco di tutti i mouse.

1. Individuare il mouse che si desidera modificare confrontando l'elenco prodotto dal comando xsetpointer con i file di configurazione /etc/X11/XF86Config o /etc/X11/xorg.conf.
2. Selezionare il mouse della console remota come mouse da modificare. Ad esempio:

   ```
   xsetpointer Mouse[2]
   ```
3. Impostare i parametri relativi alla velocità. Ad esempio:

   ```
   xset m 1/1 1
   ```

Red Hat Enterprise Linux

Impostare i parametri relativi alla velocità mediante il seguente comando:

```
xset m 1/1 1
```

Sincronizzazione del mouse in Windows®

L'impostazione predefinita High Performance mouse (Mouse ad alte prestazioni) disponibile nella pagina Global Settings (Impostazioni globali) consente di definire le impostazioni ottimali in base al sistema operativo del server. Per il corretto funzionamento, è necessario che il driver dell'interfaccia di gestione di HP ProLiant Lights-Out sia caricato e che il server sia stato riavviato dopo aver eseguito l'installazione dei driver. In caso di problemi di sincronizzazione del mouse in Windows, impostare l'opzione High Performance Mouse (Mouse ad alte prestazioni) su **Yes** (Sì).

Impostazioni del mouse ad alte prestazioni

Quando si utilizza la console remota, è possibile abilitare la funzionalità High Performance Mouse (Mouse ad alte prestazioni). La funzionalità High Performance Mouse migliora sensibilmente le prestazioni e la precisione del puntatore nei sistemi operativi supportati. Il mouse ad alte prestazioni di iLO 2 è un dispositivo di puntamento che fornisce le coordinate di posizione assolute per descrivere la relativa posizione, analogamente a un mouse USB per Tablet PC. Un mouse convenzionale invia informazioni sulla posizione relativa (ad esempio, il mouse si è spostato di 12 pixel a destra). Il computer host può modificare le informazioni sulla posizione relativa per attivare funzionalità quali l'accelerazione del mouse. Quando si utilizza la console remota, tali modifiche vengono effettuate in modo invisibile al client. La sincronizzazione tra il cursore del mouse del client e quello del mouse dell'host non può quindi essere eseguita.

Entrambe le applet della console remota integrata e della console remota inviano a iLO 2 le coordinate assolute e relative del cursore del mouse. Quando è in modalità High Performance Mouse (Mouse ad alte prestazioni), iLO 2 elimina le coordinate relative e invia le coordinate assolute all'emulatore del mouse USB per Tablet PC. In questo modo il server è in grado di "vedere" lo spostamento del mouse come se le informazioni sulle coordinate fossero state originate da un mouse USB locale per Tablet PC. Quando iLO 2 non è in modalità High Performance Mouse (Mouse ad alte prestazioni), le coordinate assolute vengono eliminate e le coordinate relative vengono inviate all'emulatore del mouse a coordinate relative USB.

La modalità High Performance Mouse (Mouse ad alte prestazioni) è disponibile solo sui sistemi operativi che supportano mouse USB per Tablet PC. Nei sistemi Windows® è necessario abilitare l'opzione High-Performance Mouse (Mouse ad alte prestazioni) nella schermata Remote Console Settings (Impostazioni console remota). Gli utenti Linux possono attivare l'opzione High Performance Mouse (Mouse ad alte prestazioni) dopo che è stato installato il driver iLO 2 High Performance Mouse per Linux. Quando si utilizzano server che eseguono altri sistemi operativi, per risolvere eventuali problemi relativi al mouse della console remota è necessario disabilitare l'opzione High Performance Mouse (Mouse ad alte prestazioni).

Quando si utilizza la console remota integrata da iLO 2 e SmartStart, il mouse locale e il mouse remoto non sono allineati. È necessario disabilitare l'opzione High Performance Mouse (Mouse ad alte prestazioni) mentre SmartStart è in esecuzione. Se, durante l'utilizzo della funzionalità High Performance Mouse, il mouse locale e il mouse remoto risultano non allineati, è possibile riallinearli utilizzando il tasto Ctrl di destra. In alternativa, è possibile utilizzare la console remota di Java™ al posto della console remota integrata.

L'opzione High Performance Mouse (Mouse ad alte prestazioni) risolve tutti i problemi di sincronizzazione del mouse nei sistemi operativi host supportati. È possibile selezionare questa modalità nella pagina Remote Console Settings (Impostazioni console remota) prima di avviare la

console remota. È tuttavia possibile che tale modalità non sia supportata da tutti i sistemi operativi, in particolare durante l'installazione. Per ottimizzare le prestazioni:

- Per aumentare il livello di prestazioni della console remota, selezionare per lo schermo del server remoto una risoluzione più bassa. La risoluzione massima supportata è 1280 x 1024 pixel.
- Per aumentare al massimo la visibilità della console remota, impostare per lo schermo del client una risoluzione più alta di quella dello schermo del server remoto.
- Le impostazioni dei colori del server remoto non influenzano in alcun modo le prestazioni della console remota. La console remota viene visualizzata con 4096 colori (12 bit).
- Sul sistema remoto utilizzare un puntatore del mouse non animato.
- Disabilitare le tracce del mouse sul sistema remoto.

Per configurare il server host, specificare le seguenti impostazioni nel Pannello di controllo:

1. Selezionare **Mouse>Puntatori>Combinazione>Predefinita di Windows**. Fare clic su **OK**.
2. Nella pagina Mouse>Puntatori selezionare **Abilita ombra puntatore**. Fare clic su **OK**.
3. Selezionare **Schermo>Impostazioni>Avanzate>Risoluzione problemi>Accelerazione hardware>Max**. Fare clic su **OK**.
4. Selezionare **Sistema>Avanzate>Impostazioni (Prestazioni)>Effetti visivi>Regola in modo da ottenere le prestazioni migliori**. Fare clic su **OK**.

In alternativa, queste impostazioni possono essere definite automaticamente dall'utility HP Online Configuration (HPONCFG). È inoltre possibile modificare le impostazioni High Performance Mouse (Mouse ad alte prestazioni) utilizzando il comando `MOD_GLOBAL_SETTINGS`. Per ulteriori informazioni sull'utilizzo del comando `MOD_GLOBAL_SETTINGS`, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

Console remota condivisa

La console remota condivisa è una funzionalità di iLO 2 che consente di connettere un massimo di quattro sessioni sullo stesso server. Questa funzionalità non sostituisce la funzionalità di acquisizione, descritta nella sezione "Acquisizione della console remota" (Acquisizione della console remota a pagina 100), e consente ai client con accesso completo (lettura/scrittura) di controllare l'alimentazione. La console remota condivisa non consente di passare una designazione host server a un altro utente né di rieseguire una connessione utente dopo che si è verificato un errore di connessione. Per consentire l'accesso utente dopo un errore, è necessario riavviare la sessione della console remota.

Questa funzionalità richiede un'apposita licenza e può essere acquistata insieme a licenze opzionali. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20).

La console remota condivisa e la modalità Forced Switch sono disabilitate per impostazione predefinita. Queste funzionalità devono essere attivate mediante il browser, SMASH CLI (OEM) o RIBCL. Tutte le sessioni della console vengono prima crittografate mediante l'autenticazione del client, quindi il responsabile della sessione decide se consentire la nuova connessione.

Il primo utente che inizializza una sessione della console remota si connette al server normalmente e viene designato come responsabile della sessione (host della sessione). Qualsiasi utente successivo che richiede l'accesso alla console remota avvia una richiesta di accesso, richiedendo una connessione client satellite, chiamando il responsabile della sessione. Per ogni richiesta di client satellite sul desktop del responsabile della sessione viene visualizzata una finestra a comparsa in cui è specificato il nome utente del richiedente e il nome DNS (se disponibile) o l'indirizzo IP.

Gli host di sessione hanno la facoltà di concedere o negare l'accesso. Nella finestra del browser della console remota viene visualizzato un elenco di utenti e nomi di host di sessione. Le sessioni client satellite vengono chiuse quando viene chiuso l'host della sessione.

Le sessioni condivise non funzionano in modo ottimale con le funzionalità Console Capture e Replay di iLO 2. Se una sessione satellite sta visualizzando una sessione acquisita, durante la durata di riproduzione la sessione satellite non riceverà i messaggi di controllo del responsabile della sessione. Se l'host della sessione inizia a visualizzare dati video acquisiti durante una sessione condivisa, il video verrà visualizzato in tutte le sessioni satellite della console remota.

Utilizzo della funzionalità Console Capture

Console Capture è una funzionalità della console remota che consente di registrare e riprodurre una sequenza video di eventi quali l'avvio, eventi ASR e errori del sistema operativo rilevati. È inoltre possibile avviare e interrompere manualmente la registrazione di video della console. Console Capture è disponibile soltanto mediante l'interfaccia utente di iLO 2 e non è possibile utilizzarla tramite scripting XML o il CLP. Console Capture è una funzionalità che richiede un'apposita licenza e può essere acquistata insieme a licenze opzionali. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20).

Per memorizzare i dati video acquisiti, nel processore di gestione è disponibile un'apposita area buffer. Questa area buffer viene condivisa con il buffer di aggiornamento del firmware. Di conseguenza, quando viene avviato il processo di aggiornamento del firmware tutte le informazioni acquisite vanno perse. Non è possibile acquisire dati video durante il processo di aggiornamento del firmware.

Lo spazio buffer è limitato. Nell'area buffer viene memorizzato un solo evento di ogni tipo di evento alla volta. È possibile trasferire in un client i buffer di dati acquisiti eseguendo la console remota integrata per la riproduzione. È inoltre possibile configurare iLO 2 per l'invio automatico a un server Web dei dati video acquisiti sulla stessa rete di iLO 2 quando si verifica un evento. In questo caso il server Web deve accettare i trasferimenti di dati con metodo POST. È possibile selezionare soltanto il buffer di avvio, soltanto il buffer degli errori o combinarli come un buffer di grandi dimensioni per disporre di maggiore spazio per l'acquisizione di sequenze di avvio di Linux.

Ai dati buffer esportati viene assegnato un nome univoco per facilitarne l'identificazione ai fini della riproduzione. La riproduzione richiede un processore iLO 2 con licenza disponibile nella rete. Alcuni sistemi operativi, ad esempio Linux, riempiono il buffer rapidamente. Se si lascia la console di sistema in modalità testo, sarà possibile aumentare al massimo la quantità di informazioni acquisite. Anche la chiusura o la riduzione del numero di elementi della console grafica attivi consente di ottimizzare lo spazio dei buffer interni.

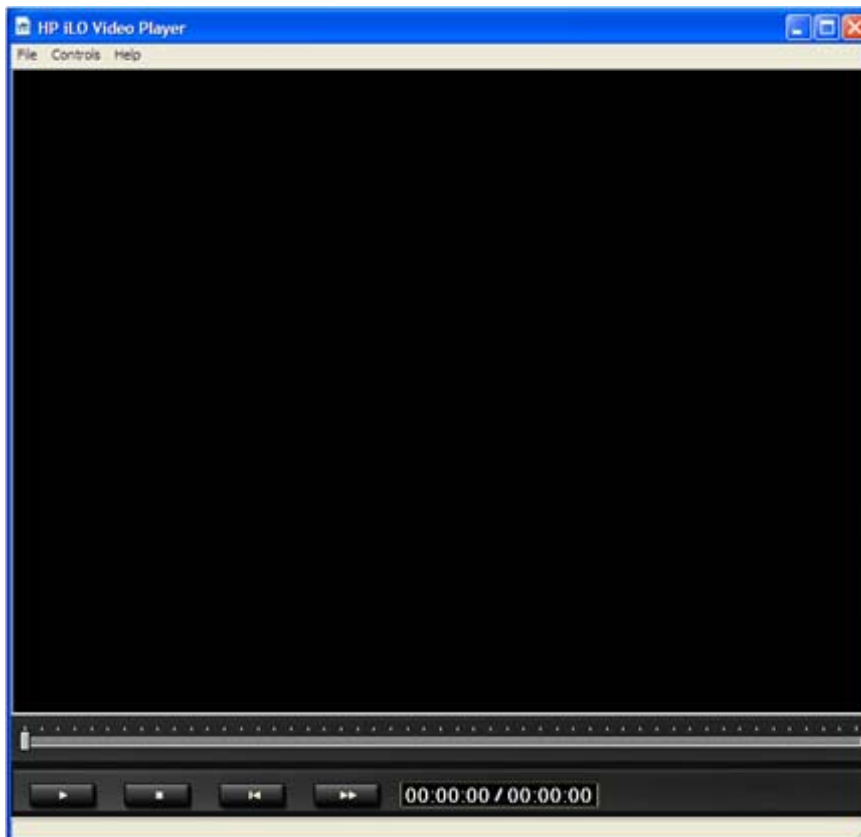
È possibile acquisire manualmente video della console del server utilizzando la funzionalità IRC Record. Tutti i dati acquisiti manualmente vengono memorizzati in un file locale sul client per essere successivamente riprodotti.

Utilizzo di HP iLO Video Player

HP iLO Video Player consente di riprodurre i file di acquisizione della console di iLO 2 senza installare iLO 2 sul sistema locale. In iLO Video Player sono disponibili controlli simili a quelli di un normale lettore di file multimediali. iLO Video Player può essere eseguito come applicazione standalone su un server o un client. In genere, l'applicazione si trova sul client. I file di acquisizione di iLO 2 vengono creati utilizzando la funzionalità Console Capture di iLO 2. Per ulteriori informazioni, vedere la sezione "Utilizzo della funzionalità Console Capture" (Utilizzo della funzionalità Console Capture a pagina 98).

Per utilizzare iLO Video Player, è necessario che sul sistema sia installato Microsoft Windows® 2000, Windows® XP o Windows Vista® e Internet Explorer (versione 6 o successiva).

Interfaccia utente di iLO Video Player

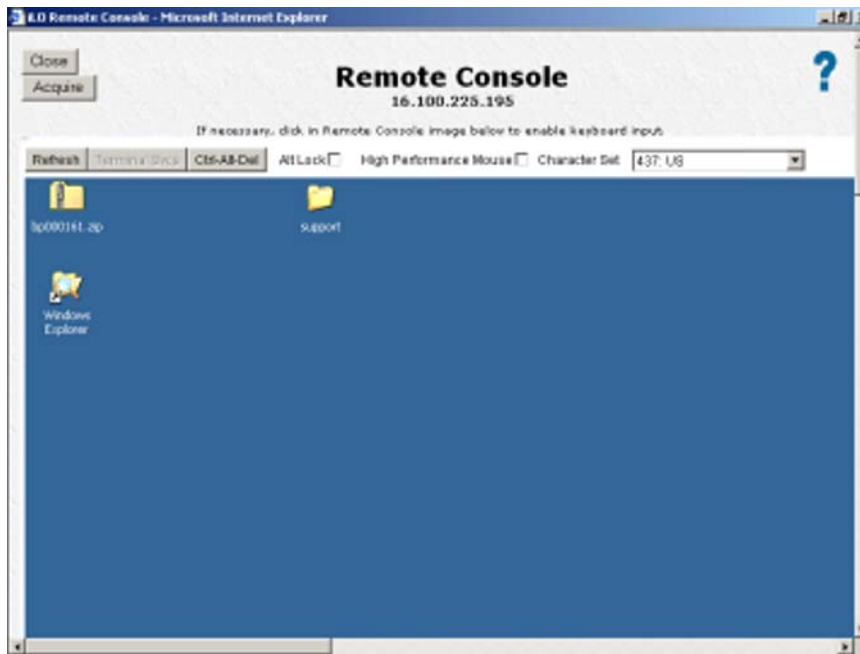
Quando si avvia HP iLO Video Player, viene visualizzata l'interfaccia utente da cui è possibile controllare tutte le funzioni di riproduzione.

Di seguito sono elencate le opzioni dei menu di iLO Video Player:

- File
  - Open (Apri) - Apre un file di acquisizione video.
  - Exit (Esci) - Chiude iLO Video Player.
- Controlli
  - Play (Riproduci) - Riproduce o riavvia il file di acquisizione video corrente.
  - Stop (Interrompi) - Interrompe la riproduzione del file di acquisizione video corrente.
  - Skip to Start (Torna all'inizio) - Riavviare la riproduzione del file di acquisizione video corrente.
  - Change Speed (Modifica velocità) - Modifica la velocità di riproduzione del file di acquisizione video corrente di iLO.
- Help (Guida in linea)
  - Help Topics (Guida) - Apre la Guida di iLO Video Player.
  - About (Informazioni) - Apre la pagina contenente le informazioni relative a iLO Video Player.

Controlli di iLO Video Player

Control (Controllo)	Nome	Funzione
	Riproduci/Pausa	Avvia la riproduzione se il file attualmente selezionato non è in esecuzione oppure è in pausa. Se la riproduzione è già in corso, il file viene messo in pausa. Se non è selezionato alcun file, il pulsante è disabilitato.
	Interrompi	Interrompe la riproduzione. Se non è selezionato alcun file, il pulsante è disabilitato.
	Torna all'inizio	Riavvia la riproduzione dall'inizio del file. Se non è selezionato alcun file, il pulsante è disabilitato.
	Cerca	Sposta la posizione corrente del video in avanti o indietro. Se non è selezionato alcun file, il pulsante è disabilitato.
	Modifica velocità	Modifica la velocità di riproduzione del file attualmente selezionato. Le velocità disponibili sono 1x, 2x, 4x, 8x e 16x. A ogni pressione viene impostata in sequenza la velocità successiva, nel seguente ordine: 2x, 4x, 8x, 16x e 1x. Se non è selezionato alcun file, il pulsante è disabilitato.
00:00:00 / 00:00:00	Posizione file	Mostra i parametri temporali del file attualmente selezionato, nel formato HH:MM:SS. • Il tempo restante nella parte sinistra indica la posizione di riproduzione corrente del file. • Il tempo nella parte destra indica la durata totale del file.

Acquisizione della console remota

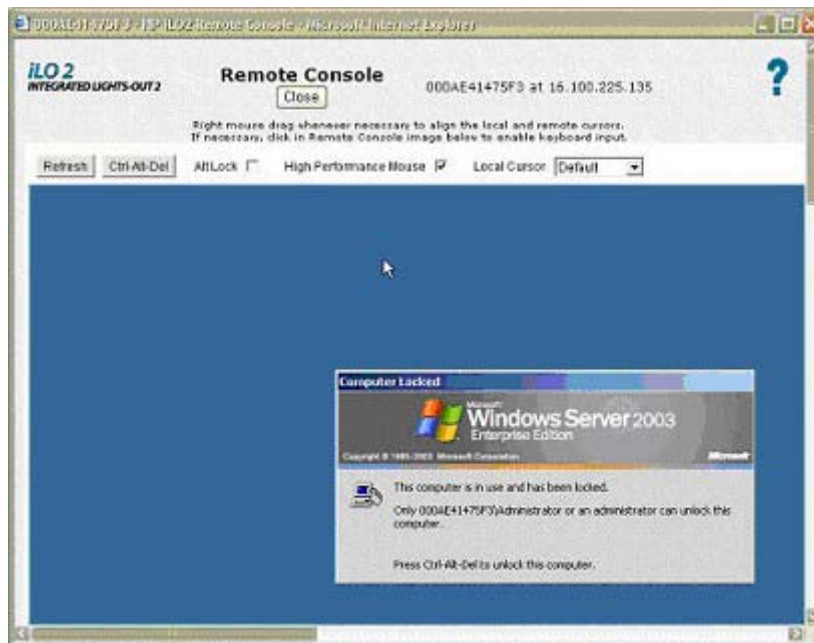
Quando l'impostazione Remote Console Acquire (Acquisizione console remota) disponibile nella schermata Remote Console Settings (Impostazioni console remota) è abilitata, nella pagina Remote Console (Console remota) viene visualizzato il pulsante Acuire (Acquisisci). Se all'apertura della pagina della console remota viene segnalato che un altro utente sta attualmente utilizzando la console remota, facendo clic sul pulsante Acquire (Acquisisci) è possibile terminare la sessione di utilizzo della console remota dell'altro utente e avviarne una nuova nella finestra corrente.

Quando si fa clic sul pulsante Acquire (Acquisisci) viene chiesto di confermare l'interruzione della sessione di utilizzo della console remota dell'altro utente. L'altro utente riceverà un avviso che un altro utente ha acquisito la sessione della console remota dopo l'interruzione della connessione. Non viene fornito alcun avviso preliminare. Dopo aver confermato che si desidera procedere con l'operazione di acquisizione, verrà visualizzata una finestra di avviso in cui è indicato che per completare l'operazione può essere necessario un periodo di tempo superiore a 30 secondi. Il pulsante Acquire (Acquisisci) risulta disabilitato non appena si fa clic su di esso e l'operazione di acquisizione viene avviata. Nei browser che lo supportano, il pulsante verrà visualizzato in grigio chiaro per indicare che è disabilitato. In altri browser è possibile che non sia disponibile alcuna indicazione visiva della disabilitazione del pulsante.

Il comando di acquisizione può essere utilizzato solo una volta ogni cinque minuti da qualsiasi utente. Se un altro utente ha recentemente acquisito la console remota e si seleziona il pulsante Acquire (Acquisisci), è possibile che venga segnalato che è in corso il periodo di disattivazione di cinque minuti della funzione di acquisizione. Chiudere la finestra e avviare di nuovo la console remota. Nella nuova pagina il pulsante Acquire (Acquisisci) sarà disabilitato fino al termine del periodo di disattivazione della funzione di acquisizione. Quando il pulsante Acquire (Acquisisci) viene abilitato (si tratta di un processo automatico pertanto non è necessario aggiornare la pagina), è possibile tentare di acquisire nuovamente la sessione della console remota. Nei browser che lo supportano, il pulsante verrà visualizzato in grigio chiaro per indicare che è disabilitato durante questo periodo di cinque minuti. In altri browser è possibile che non sia disponibile alcuna segnalazione visiva che indichi che il pulsante è disabilitato e non sarà quindi disponibile alcuna segnalazione visiva per indicare lo scadere del periodo di timeout.

È ammesso un solo tentativo di acquisizione per ogni finestra di sessione della console remota. Se l'acquisizione della console remota è stata completata e successivamente un altro utente acquisisce la console remota, è necessario aprire una nuova finestra della console remota per tentare di acquisire nuovamente la sessione.

Console remota

La console remota è un'applet Java™ in grado di offrire un'ampia compatibilità browser, inclusi i browser Windows® e Linux. I browser supportati sono elencati nella sezione "Browser e sistemi operativi client supportati" (Browser e sistemi operativi client supportati a pagina 6). Questa funzionalità richiede

un'apposita licenza e può essere acquistata insieme a licenze opzionali. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20).

Nella console remota vengono utilizzati due cursori per facilitare la distinzione tra i puntatori dei mouse locale e remoto. Il cursore del mouse del computer client viene visualizzato nella console remota come un simbolo a forma di croce. Per ottenere prestazioni ottimali, assicurarsi di configurare lo schermo del sistema operativo host come descritto nelle sezioni "Impostazioni consigliate per il client" (Impostazioni consigliate per il client a pagina 103) e "Impostazioni consigliate per il server" (Impostazioni consigliate per il server a pagina 103).

Per sincronizzare i cursori locale e remoto, effettuare una delle seguenti operazioni:

- Fare clic con il pulsante destro del mouse, trascinare e spostare il cursore locale a forma di mirino per allinearlo al cursore del mouse del server remoto.
- Tenere premuto il tasto **Ctrl** di destra, quindi spostare il cursore a forma di mirino del client locale in modo da allinearlo al cursore del mouse del server remoto.

Il cursore locale assume la forma del cursore remoto. Se il cursore locale e quello remoto sono perfettamente allineati e l'accelerazione hardware del server gestito è impostata sul valore massimo, viene visualizzato un unico cursore.

Funzionalità e controlli della console remota

Nell'applet della console remota sono disponibili alcuni pulsanti che offrono a iLO 2 l'accesso e il controllo di funzionalità avanzate. Sono disponibili le seguenti opzioni:

- Refresh (Aggiorna) consente di eseguire l'aggiornamento dello schermo di iLO 2.
- Terminal Svcs (Servizi terminal) avvia il client di Servizi terminal Microsoft® installato nel sistema. Se i Servizi terminal sono disabilitati o non installati sul server, questo pulsante risulterà disattivato.
- Ctrl-Alt-Del invia la sequenza di tasti Ctrl+Alt+Canc alla console remota.
- Alt Lock (Blocco Alt), se selezionato, determina l'invio di qualsiasi pressione di tasto al server, come quando vengono premuti contemporaneamente Alt e un altro tasto.

- Character Set (Set di caratteri) consente di modificare il set di caratteri predefinito utilizzato dalla console remota. Modificando il set di caratteri della console remota si garantisce una corretta visualizzazione dei caratteri.
- Close (Chiudi) termina la sessione e chiude la finestra della console remota.

Impostazioni consigliate per il client

La risoluzione dello schermo del sistema operativo del server remoto dovrebbe essere preferibilmente identica o inferiore a quella del computer del browser. Risoluzioni più elevate consentono di trasmettere maggiori informazioni, ma rallentano le prestazioni generali.

Per ottimizzare le prestazioni, utilizzare le seguenti impostazioni per il client e il browser:

- **Display Properties (Proprietà di visualizzazione)**
  - Selezionare un valore superiore a 256 colori.
  - Selezionare una risoluzione maggiore di quella dello schermo del server remoto.
  - Proprietà dello schermo di Linux X: nella finestra X Preferences (Preferenze X), impostare la dimensione del carattere su **12**.
- **Remote Console (Console remota)**
  - Per la velocità della console remota si consiglia di utilizzare un client a 700 MHz o più veloce, con almeno 128 MB di memoria.
  - Per l'esecuzione dell'applet Java™ della console remota si consiglia di utilizzare un client con un solo processore.
- **Mouse Properties (Proprietà del mouse)**
  - Impostare la velocità del puntatore mouse sul valore medio.
  - Impostare l'opzione Mouse Pointer Acceleration (Accelerazione puntatore del mouse) su low (bassa) oppure disabilitare l'accelerazione del puntatore.

Impostazioni consigliate per il server

Di seguito è riportato l'elenco delle impostazioni consigliate per il server a seconda del sistema operativo utilizzato.

NOTA: Per visualizzare l'intera schermata del server host sull'applet della console remota del server, impostare la risoluzione dello schermo del server su un valore uguale o inferiore alla risoluzione del client.

Impostazioni di Microsoft® Windows® Server 2003

Per ottimizzare le prestazioni, per il server non selezionare alcuno sfondo in **Display Properties** (Proprietà dello schermo) e in **Mouse Properties** (Proprietà del mouse) impostare **Disable Pointer Trails** (Disabilita traccia del puntatore).

Impostazioni per server Red Hat Linux e SUSE Linux

Per ottimizzare le prestazioni, nelle proprietà del mouse del server impostare la velocità del puntatore su **1x**. Per KDE, accedere a **Control Center** (Centro di controllo), selezionare **Peripherals/Mouse** (Periferiche/Mouse), quindi selezionare la scheda **Advanced** (Avanzate).

Panoramica sulla console remota basata su testo

iLO e i relativi predecessori supportano una vera e propria console remota basata su testo. Le informazioni video vengono ottenute dal server e il contenuto della memoria video viene inviato al processore di gestione, compresso, crittografato e inoltrato all'applicazione client di gestione. iLO utilizza un buffer di frame dello schermo in grado di rilevare le modifiche nelle informazioni di testo, crittografare tali modifiche e inviare i caratteri (incluse le informazioni di posizionamento sullo schermo) alle applicazioni client basate su testo. Questo metodo garantisce la compatibilità con client standard basati su testo, buone prestazioni e semplicità d'uso. Non è tuttavia possibile visualizzare informazioni grafiche o non ASCII. È inoltre possibile che le informazioni di posizionamento sullo schermo (i caratteri visualizzati) non vengano inviate nell'ordine corretto.

La console remota utilizza la tecnologia Virtual KVM e non fornisce una vera e propria console basata su testo. iLO 2 utilizza la porta DVO per adattatori video per accedere direttamente alla memoria video. Questo metodo consente di migliorare notevolmente le prestazioni di iLO 2. Tuttavia, il flusso di dati video digitali non contiene dati testuali utili. I dati ottenuti dalla porta DVO rappresentano dati grafici (non basati su caratteri) e non dati ASCII o testuali comprensibili. Di conseguenza, non possono essere visualizzati in un'applicazione client basata su testo quale telnet o SSH.

Console di testo durante il POST

La console remota basata su testo di iLO 2 standard rimane disponibile in iLO 2 fino al termine del POST del sistema operativo. Il firmware standard di iLO 2 continua a utilizzare la funzionalità della porta seriale virtuale del processore di gestione. Sul firmware di iLO 2, la porta seriale virtuale è stata rinominata console seriale remota. iLO 2 utilizza la console seriale remota per accedere a una console remota basata su testo prima dell'avvio del sistema operativo. L'applet della console seriale remota di iLO 2 appare come una console basata su testo, ma le informazioni vengono visualizzate tramite dati grafici. iLO 2 visualizza queste informazioni tramite l'applet della console remota prima dell'avvio del sistema operativo del server, consentendo a un processore di gestione iLO 2 senza licenza di osservare il server e interagire con esso durante le attività di POST.

Per un blade iLO 2, e un blade iLO che esegue Linux in formato grafico, immettere `getty()` sulla porta seriale del server, quindi utilizzare la console seriale remota di iLO 2 o la porta seriale virtuale di iLO (comando CLP `start /system1/oemhp_vsp1`) per visualizzare una sessione di accesso al sistema operativo Linux tramite la porta seriale.

Un processore iLO 2 senza licenza non può utilizzare l'accesso tramite console remota dopo il completamento del POST e l'avvio del sistema operativo. Per poter utilizzare la console remota e la console di testo iLO dopo il POST, è necessaria una licenza iLO 2 Advanced o iLO 2 Advanced for Blade System.

Console di testo dopo il POST

La funzionalità della console di testo iLO 2 dopo il POST è una console basata su testo accessibile da telnet o SSH dopo il POST. Quando si utilizza SSH, il flusso dati, incluse le credenziali di autenticazione, viene protetto dal metodo di crittografia supportato dal client SSH e iLO 2. HP consiglia l'utilizzo di SSH per la connessione alla console di testo iLO 2.

iLO 2 supporta anche l'utilizzo di telnet per la connessione alla console di testo iLO 2. In questo caso, tuttavia, il flusso dati non viene crittografato. Nel criterio di protezione predefinito, l'utilizzo di telnet è disabilitato. È necessario abilitare telnet per consentire l'accesso all'interfaccia CLI e alla console di testo iLO 2.

Per ulteriori informazioni sulla protezione dei metodi di comunicazione utilizzati da iLO 2, vedere *Integrated Lights-Out security technology brief* (Articolo tecnico sulla protezione di Integrated Lights-Out) sul sito Web HP (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00212796/c00212796.pdf).

La presentazione di colori, caratteri e controlli dello schermo dipende dal client utilizzato, che può essere un qualsiasi client SSH o telnet (se abilitato) standard compatibile con iLO 2. Per impostazione predefinita, la console di testo iLO 2 è abilitata sul firmware di iLO 2 versione 1.50 e successive. Di seguito sono indicate le funzionalità supportate:

- Visualizzazione di schermate in modalità testo 80x25 (configurazioni di colore standard) quando il sistema è acceso, inclusi:
  - Processo di avvio del sistema (POST)
  - ROM opzionali standard
  - Caricatori di avvio in modalità testo (LiLO o GRUB)
  - Sistema operativo Linux in modalità VGA 80x25
  - DOS
  - Altri sistemi operativi basati su testo

    Il supporto delle schermate in modalità testo non include grafici, altre risoluzioni di testo VGA (132x48, 80x48) né altre risoluzioni di testo implementate mediante un driver (implementazione a livello grafico).
- Tasti di scelta rapida della console remota
- Tastiere internazionali (se il server e il client sono configurati in modo simile)
- Caratteri di disegno, purché nell'applicazione client siano selezionati il carattere e la tabella codici corretti

Per poter utilizzare la funzionalità della console di testo iLO 2, è necessario aggiornare la ROM HOST. iLO 2 supporta la console di testo iLO 2 sui server HP ProLiant BL460c G1, BL480c G1, ML350 G5, DL360 G5, ML370 G5, DL380 G5, BL680 G5 e DL580 G5.

Utilizzo della console di testo iLO

Per avviare una sessione di console di testo iLO 2:

1. Avviare una sessione SSH o telnet.

   Assicurarsi che la codifica caratteri dell'applicazione di terminale sia impostata su Western (ISO-8859-1) (Occidentale (ISO-8859-1)).
2. Accedere a iLO 2.
3. Al prompt, immettere `textcons`.

   Viene visualizzato un messaggio per indicare che è in corso l'inizializzazione del software della console di testo iLO 2.

Per chiudere una console di testo iLO 2 e tornare alla sessione CLI, premere contemporaneamente i tasti **ESC (**.

Personalizzazione della console di testo iLO 2

Quando si avvia la console di testo iLO 2, utilizzare le opzioni e gli argomenti del comando `textcons` per personalizzare il funzionamento della schermata. In genere, non è necessario modificare queste opzioni.

- Controllo della velocità di campionamento

  È possibile utilizzare l'opzione `textcons speed` per indicare, in millisecondi, la frequenza dei periodi di campionamento. Per periodo di campionamento si intende il periodo in cui il firmware di iLO 2 esamina le modifiche dello schermo e aggiorna la console di testo iLO 2. La regolazione della velocità consente di eliminare il traffico inutile nei collegamenti di rete lunghi o lenti nonché ridurre l'ampiezza di banda utilizzata e il tempo di CPU iLO 2 consumato. I valori accettabili sono compresi tra 1 e 5000 (da 1 ms a 5 secondi). Ad esempio:

  ```
  textcons speed 500
  ```

- Controllo della stabilità (smoothing)

  iLO tenta di trasmettere i dati solo quando cambiano e diventano stabili nella schermata. Se una riga della schermata di testo cambia costantemente a una velocità maggiore rispetto a quella di campionamento di iLO 2, la riga non viene trasmessa fino a quando non diventa stabile. Ad esempio, durante l'esecuzione di un comando `ls -R` su un file system di grandi dimensioni, il testo viene visualizzato sul monitor troppo rapidamente per poter essere interpretato. La stessa situazione si verifica in una sessione di console di testo iLO 2. In questo caso, i dati vengono visualizzati rapidamente e non sono decifrabili. In questo caso, tuttavia, i dati vengono trasmessi da iLO 2 sulla rete, con conseguente consumo dell'ampiezza di banda. Il comportamento predefinito è "smoothing" (delay 0), che prevede la trasmissione dei dati solo quando le modifiche diventano stabili. È possibile controllare o disabilitare la funzionalità di smoothing utilizzando l'opzione delay. Ad esempio:

  ```
  textcons speed 500 delay 10
  ```

- Controllo del supporto per tastiere internazionali

  Quando si utilizza la console di testo iLO 2, iLO 2 può emulare il mapping dei caratteri tra il client, telnet e il server. Il mapping predefinito è la conversione di tastiera USB 101 (ovvero nessuna conversione).

  Per controllare la conversione, utilizzare l'opzione `xlt` con il numero di riferimento appropriato. Ad esempio, per impostare la console di testo iLO 2 con una velocità di campionamento di 50 ms utilizzando la conversione di una tastiera britannica, immettere:

  ```
  textcons speed 50 xlt 41
  ```

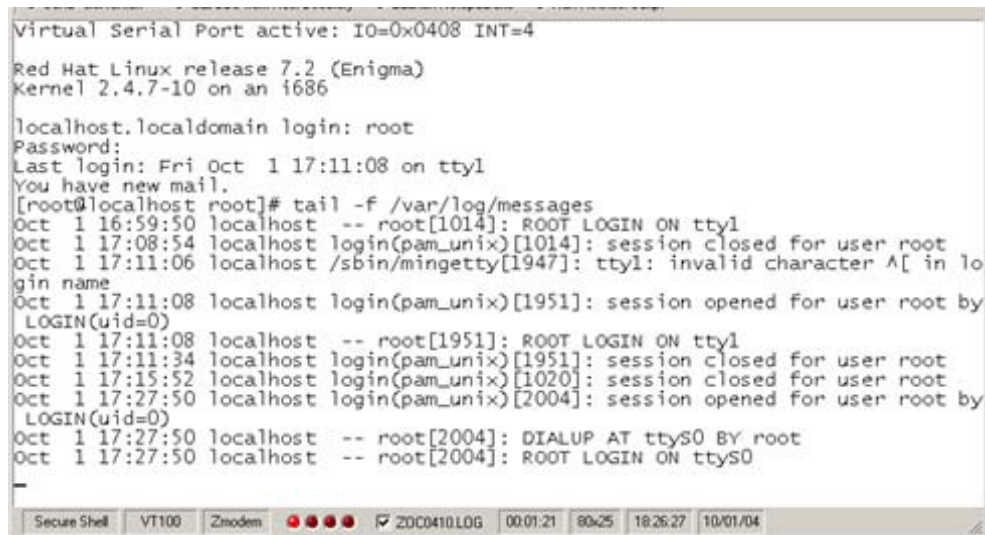
  Per la conversione in un'altra lingua, fare riferimento alla seguente tabella:

Keyboard (Tastiera)	Numero di riferimento
Stato Uniti	0
Inglese (Gran Bretagna)	1
Belga	2
Danese	3
Finlandese	4
Francese	5
Francese Canadese	6

Keyboard (Tastiera)	Numero di riferimento
Tedesco	7
Italiano	8
Latino-americano	9
Norvegese	10
Portoghese	11
Spagnolo	12
Svedese	13
Francese (Svizzera)	14
Tedesco (Svizzera)	16

- Configurazione dei tasti di scelta rapida della console remota

  Per consentire di utilizzare sequenze di tasti speciali che non possono essere duplicate nel client della console remota, i tasti di scelta rapida configurati per la console remota funzionano anche nella console di testo iLO 2. Per ulteriori informazioni, vedere la sezione "Tasti di scelta rapida della console remota" (Tasti di scelta rapida della console remota a pagina 90).

- Configurazione del mapping dei caratteri

  In generale, nel set di caratteri ASCII, i caratteri di CONTROLLO (caratteri ASCII con valore minore di 32) non sono stampabili e non possono essere visualizzati. Questi caratteri possono essere utilizzati per rappresentare elementi quali frecce, stelle o cerchi. Alcuni di questi caratteri sono mappati in rappresentazioni ASCII equivalenti, come indicato nella seguente tabella.

Valore carattere	Descrizione	Carattere equivalente mappato
0x07	Puntino	*
0x0F	Sole	*
0x10	Puntatore destro	>
0x11	Puntatore sinistro	<
0x18	Freccia su	^
0x19	Freccia giù	v
0x1A	Freccia sinistra	>
0x1B	Freccia destra	>
0x1E	Puntatore su	^
0x1F	Puntatore giù	v
0xFF	Blocco ombreggiato	spazio vuoto

Utilizzo di una sessione Linux

È possibile eseguire una porta seriale virtuale di iLO 2 in un sistema Linux, se il sistema è configurato per mostrare una sessione di terminale sulla porta seriale. Questa funzionalità consente di utilizzare un servizio di registrazione remoto. È possibile accedere in remoto alla porta seriale e reindirizzare l'output

verso un file di registro. In questo modo, tutti i messaggi di sistema diretti alla porta seriale verranno registrati in remoto.

```
Virtual Serial Port active: IO=0x0408 INT=4

Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686

localhost.localdomain login: root
Password:
Last login: Fri Oct  1 17:11:08 on tty1
You have new mail.
[root@localhost root]# tail -f /var/log/messages
Oct  1 16:59:50 localhost  -- root[1014]: ROOT LOGIN ON tty1
Oct  1 17:08:54 localhost login(pam_unix)[1014]: session closed for user root
Oct  1 17:11:06 localhost /sbin/mingetty[1947]: tty1: invalid character ^[ in lo
gin name
Oct  1 17:11:08 localhost login(pam_unix)[1951]: session opened for user root by
 LOGIN(uid=0)
Oct  1 17:11:08 localhost  -- root[1951]: ROOT LOGIN ON tty1
Oct  1 17:11:34 localhost login(pam_unix)[1951]: session closed for user root
Oct  1 17:15:52 localhost login(pam_unix)[1020]: session closed for user root
Oct  1 17:27:50 localhost login(pam_unix)[2004]: session opened for user root by
 LOGIN(uid=0)
Oct  1 17:27:50 localhost  -- root[2004]: DIALUP AT ttyS0 BY root
Oct  1 17:27:50 localhost  -- root[2004]: ROOT LOGIN ON ttyS0
_
```

Secure Shell | VT100 | Zmodem | ZOC0410.LOG | 00:01:21 | 80x25 | 18:26:27 | 10/01/04

Alcune modalità testo di Linux sono in realtà modalità grafiche e non possono essere visualizzate utilizzando la console di testo iLO 2. Ad esempio, i terminali SLES utilizzano una modalità testo su grafica. Quindi, anche se sembrano basati su testo, non vengono visualizzati correttamente nella console di testo iLO 2. Se si tenta di utilizzare una modalità non supportata, nella console di testo iLO 2 viene visualizzato un messaggio per indicare che il server sta utilizzando una modalità grafica.

È possibile che alcune sequenze di caratteri richieste da Linux in modalità testo non riescano a passare attraverso la console di testo iLO 2. Ad esempio, la combinazione di tasti ALT + TAB potrebbe essere intercettata dal client. Per ovviare a questi problemi, è possibile configurare un tasto di scelta rapida per la combinazione di tasti. Per ulteriori informazioni, vedere la sezione "Tasti di scelta rapida della console remota" (Tasti di scelta rapida della console remota a pagina 90).

Porta seriale virtuale e console seriale remota

Il processore di gestione contiene hardware di porta seriale che può sostituire la porta seriale fisica sulla scheda madre del server. Tramite un interruttore elettronico, il firmware di iLO 2 disconnette la porta seriale fisica del server e attiva la connessione del proprio hardware di porta seriale. Quest'ultimo stabilisce una connessione tra il server e la rete del processore di gestione. Il firmware incapsula i caratteri inviati dal server alla porta seriale in pacchetti di rete e invia questi ultimi all'applet della console seriale remota o all'applicazione, che può essere un client telnet o SSH. I caratteri inviati dall'applicazione o dall'applet remota vengono incapsulati in pacchetti di rete e inviati al firmware di iLO 2, che si occupa di estrarli e inviarli al server. La console seriale remota di iLO 2 fornisce un percorso di comunicazione seriale bidirezionale tra l'utente remoto e il server.

Tramite questa console, l'utente remoto può eseguire varie operazioni, ad esempio interagire con la sequenza di POST e la sequenza di avvio del sistema operativo del server, stabilire una sessione di accesso con il sistema operativo, interagire con il sistema operativo, nonché eseguire applicazioni sul sistema operativo e interagire con esse. Gli utenti del sistema operativo Microsoft® Windows Server™ 2003 possono eseguire il sottosistema EMS tramite la console seriale remota. EMS è utile per il debug dell'avvio e dei problemi a livello di kernel del sistema operativo.

Console seriale remota

Con la console seriale remota è possibile accedere a una console seriale VT320 da una console basata sull'applet Java™ collegata alla porta seriale virtuale di iLO 2 mediante un browser. L'avvio della console seriale remota consente di scambiare i dati di testo con l'host. L'opzione Remote Serial Console

(Console Seriale Remota) è compatibile con entrambi i sistemi operativi host Windows® e Linux e richiede JVM.

Il flusso di dati è un flusso bidirezionale inviato alla porta seriale del server. Su una porta seriale del server HP ProLiant possono essere visualizzati tre tipi di dati:

- Console Windows® EMS
- Sessione utente Linux tramite TTY seriale (ttyS0)
- Finestra di dialogo POST di sistema (se il reindirizzamento della console seriale BIOS è abilitato)

La configurazione corrente viene visualizzata nella pagina Remote Console Information (Informazioni console remota) quando si fa clic sulla scheda Remote Console (Console remota). Le impostazioni correnti possono essere modificate utilizzando l'utility RBSU del sistema host alla quale è possibile accedere durante un ripristino del server.

Configurazione della console seriale remota

Per utilizzare la console seriale remota, è necessario configurare il software e il firmware del server in modo appropriato. Per configurare il firmware POST del server, è necessario richiamare l'utility RBSU del server per impostare i parametri della porta seriale. Per attivare la modalità BIOS Serial Console Redirection (Reindirizzamento della console seriale BIOS) è necessario configurare l'utility RBSU. Questa modalità indica alla ROM di sistema del server di inviare e ricevere dati mediante la porta seriale del server. Quando viene attivata la modalità Remote Serial Console (Console seriale remota) del firmware di iLO 2, anziché la porta seriale del server iLO 2 attiva una porta seriale, intercetta e trasmette i dati in uscita al client della console seriale remota, riceve i dati in entrata (dal client della console seriale remota) e li ritrasmette alla ROM del sistema.

Dopo che il server ha completato il POST, la ROM di sistema del server trasferisce il controllo al caricatore di avvio del sistema operativo. Se si utilizza Linux, è possibile configurare il caricatore di avvio del sistema operativo in modo che interagisca con la porta seriale del server anziché con la tastiera, il mouse e la console VGA. Questa configurazione consente di visualizzare e interagire con la sequenza di avvio del sistema operativo mediante la console seriale remota. Per un esempio di caricatore di avvio

del sistema operativo Linux, vedere la sezione "Esempio di configurazione Linux" (Esempio di configurazione Linux a pagina 110).

Al termine del processo del caricatore di avvio del sistema operativo, il sistema operativo continua il processo di caricamento. Se si utilizza un sistema operativo Linux, è possibile configurare il sistema operativo per fornire una sessione di accesso al sistema attraverso la porta seriale, consentendo alla console seriale remota di richiedere l'ID utente e la password di accesso al sistema. L'utilizzo di questa configurazione consente di interagire con il sistema operativo come un utente o un amministratore del sistema.

Sebbene l'utilizzo della console seriale remota (rispetto all'utilizzo della console remota o della console remota integrata) richieda ulteriori operazioni di configurazione, la console seriale remota consente agli utenti Telnet o SSH di interagire con il server in remoto e senza richiedere l'utilizzo di una licenza iLO 2 Advanced. Rappresenta inoltre l'unico modo in cui una console remota basata su un vero e proprio protocollo di testo viene presentata da iLO 2.

Esempio di configurazione Linux

Il caricatore di avvio è l'applicazione che esegue il caricamento dal dispositivo di avvio quando la ROM di sistema del server completa il POST. Per i sistemi operativi Linux, il caricatore di avvio generalmente utilizzato è GRUB. Per configurare GRUB per l'utilizzo della console seriale remota, modificare il file di configurazione di GRUB in modo che risulti simile all'esempio riportato di seguito (esempio di Red Hat Linux 7.2):

```
serial -unit=0 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2) /grub/splash.zpm.gz
title Red Hat Linux (2.4.18-4smp)

root (hd0,2)
kernel /vmlinuz-2.4.18-4smp ro root=/dev/sda9 console=tty0
console=ttyS0,115200
initrd /initrd-2.4.18-rsmp.img
```

Dopo l'avvio di Linux, una console di accesso può essere reindirizzata alla porta seriale. I dispositivi /dev/ttyS0 e /dev/ttyS1, se configurati, consentono di ottenere sessioni TTY seriali attraverso la console seriale remota. Per avviare una sessione shell su una porta seriale configurata, aggiungere la seguente riga al file /etc/inittab per avviare automaticamente il processo di accesso durante l'avvio del sistema (nell'esempio riportato viene richiamata la console di accesso su /dev/ttyS0):

```
Sx:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
```

Per ulteriori informazioni sulla configurazione di Linux per l'utilizzo con la console seriale remota, consultare il manuale tecnico *Integrated Lights-Out Virtual Serial Port configuration and operation HOWTO* (Istruzioni sull'utilizzo e la configurazione della porta seriale virtuale di HP Integrated Lights-Out) disponibile sul sito Web HP all'indirizzo http://www.hp.com/servers/lights-out.

Miglioramenti apportati alla porta seriale virtuale

La versione 1.35 del firmware di iLO 2 implementa un flag dinamico che informa immediatamente la ROM di sistema del server quando viene stabilita una connessione alla console seriale remota di iLO 2. Una volta che il codice POST della ROM di sistema riconosce la connessione alla console seriale remota, il sistema inizia a reindirizzare l'input e l'output della console alla porta seriale del server e alla console seriale remota. È possibile avviare una sessione della console seriale remota in qualsiasi momento prima o durante la sequenza del POST di sistema, nonché visualizzare e modificare il POST. Dopo la disconnessione della sessione della console seriale remota, il firmware di iLO 2 reimposta il

flag dinamico per informare la ROM di sistema del server che la sessione non è più attiva. La ROM di sistema del server annulla quindi il reindirizzamento alla porta seriale del server.

Per utilizzare la porta seriale virtuale di iLO 2 e rendere operativo questo miglioramento, è necessario configurare l'utility RBSU della ROM di sistema. Per ulteriori informazioni, vedere la sezione "Configurazione della console seriale remota" (Configurazione della console seriale remota a pagina 109).

Console Windows® EMS

Se è abilitata, la console Windows® EMS consente di usare i servizi di gestione emergenze (EMS) nei casi in cui non sia possibile usare normalmente lo schermo, i driver dei dispositivi o altre funzioni del sistema operativo, né le normali azioni correttive relative.

iLO 2 consente però di usare questi servizi in rete tramite un browser Web. Microsoft® EMS permette di visualizzare i processi in esecuzione, modificare la priorità dei processi e bloccare questi ultimi. È possibile usare contemporaneamente la console EMS e la console remota di iLO 2.

La porta seriale di Windows® EMS deve essere abilitata attraverso l'utility RBSU del sistema host. Mediante la configurazione è possibile abilitare o disabilitare la porta EMS e la selezione della porta COM. Il sistema iLO 2 rileva automaticamente lo stato della porta EMS (abilitata o disabilitata) e la selezione della porta COM.

Per visualizzare il prompt `SAC>` potrebbe essere necessario premere `Invio` dopo aver effettuato la connessione tramite la console della porta seriale virtuale.

Per ulteriori informazioni sull'uso delle funzioni EMS, consultare la documentazione di Windows® Server 2003.

Utilizzo della funzione Virtual Serial Port in modalità raw

È possibile utilizzare la funzione Virtual Serial Port di iLO 2 per connettere un debugger del kernel di Windows® da un client remoto mediante l'utility WiLODbg.exe, che consente di ignorare la decodifica dei byte da parte del firmware di iLO 2. Una volta ignorata la decodifica dei byte, la funzione Virtual Serial Port viene eseguita in modalità RAW (non elaborata) e inviata direttamente alla porta seriale.

L'utility WiLODbg.exe viene eseguita su un sistema client in cui è installata l'applicazione Microsoft® WinDBG.exe o KD.exe. Quando si esegue WiLODbg.exe, viene automaticamente stabilita una connessione tra iLO 2 e la porta seriale virtuale e viene abilitata la modalità RAW. Viene inoltre avviato il file WinDBG.exe, insieme agli switch necessari per consentirne la connessione al dispositivo iLO 2 remoto.

Per configurare il server, è necessario configurare l'utility RBSU del sistema:

1. Per abilitare una porta seriale virtuale, assegnare alla funzione Virtual Serial Port (Porta seriale virtuale) una porta COM dal menu System Options (Opzioni di sistema).
2. Impostare le opzioni BIOS Serial Console Port (Porta console seriale del BIOS) e EMS Console (Console EMS) su **Disable** (Disabilita) o impostarle sulla stessa porta dell'opzione Embedded Serial Port (Porta seriale incorporata).
3. Impostare la porta di Microsoft® Windows® Debug sulla stessa porta della funzione Virtual Serial Port (Porta seriale virtuale). A questo scopo, è possibile utilizzare il comando `bootcfg` oppure modificare il file boot.ini.

   Esempio di utilizzo del comando `bootcfg`:

   Al prompt dei comandi di un server Windows®, immettere il seguente comando:

   ```
   Bootcfg /debug on /port com2 /baud 115200 /id 1
   ```

Esempio di file boot.ini modificato:

```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Debug (com2)" /
fastdetect /debug /debugport=com2 /baudrate=115200
```

Se il server è stato configurato per l'avvio in modalità debug e durante l'avvio del server viene stabilita una connessione normale alla porta seriale virtuale, alcuni byte dei dati di debug vengono inviati al client della porta seriale virtuale. Per impedire il verificarsi di questa situazione, evitare di avviare il server in modalità debug mentre è attiva una connessione normale alla porta seriale virtuale.

La funzione Serial Port Configuration (Configurazione porta seriale) visualizza le informazioni sulla configurazione del server, le porte seriali disponibili e lo stato della porta seriale virtuale. Lo stato può essere impostato su:

- Available (Disponibile) – La porta seriale virtuale non è in uso.
- In use (In uso) – In modalità normale se è stata stabilita una connessione normale alla porta seriale virtuale.
- In use (In uso) – In modalità Raw se la connessione è stata effettuata mediante l'utility WiLODbg.exe.

Quando la porta seriale virtuale è in uso, il pulsante Disconnect (Disconnetti) è attivo e può essere utilizzato per terminare qualsiasi tipo di connessione alla porta seriale virtuale. Se si utilizza Disconnect (Disconnetti) per interrompere una connessione alla porta seriale virtuale stabilita mediante SSH, la connessione SSH viene terminata e non viene visualizzato il prompt `</>hpiLO->`. La stessa situazione si verifica se la connessione alla porta seriale virtuale è stata stabilita mediante telnet. Se invece la connessione è stata effettuata da un browser utilizzando un'applet per la connessione seriale remota, l'applet viene disconnessa. Per ristabilire la connessione seriale virtuale, è necessario chiudere e riaprire la finestra dell'applet.

Utilizzo di un debugger del kernel di Windows remoto

Per avviare un debugger del kernel di Windows®, è necessario avviare l'utility WiLODbg.exe su un client in cui sia installato Microsoft® WinDBG.exe o KD.exe, quindi riavviare il server remoto in modalità debug per collegare il debugger. WiLODbg lancia automaticamente il file WinDBG.exe o KD.exe. Ad esempio:

```
WiLODbg <IP Address>[ -c CommandLine][ -e][ -k][ -p Password][ -s
SocketNumber][
-t][ -u Username]
If a parameter has whitespace in it, enclose it in quotes.
```

Parametri obbligatori:

`IP Address = <String>`: indirizzo IP in formato "dot" o nome UNC completo. <String> è costituito da una serie di caratteri. I parametri richiesti devono essere inseriti nell'ordine riportato nell'esempio.

Parametri opzionali:

- -c CommandLine = <String>: fornisce parametri della riga di comando aggiuntivi per il debugger selezionato. Se il parametro contiene trattini (-) o spazi incorporati, racchiuderlo tra virgolette. <String> è costituito da una serie di caratteri.
- -e = <Boolean>: attiva la crittografia per il collegamento di comunicazione. In questa versione, la crittografia può essere attivata solo se si utilizzano connessioni telnet. Per impostazione predefinita, la crittografia è disabilitata.
- -k = <Boolean>: consente di utilizzare KD anziché WinDbg. Per impostazione predefinita, viene utilizzato WinDbg.
- -p Password = <String>: imposta la password da utilizzare per l'accesso a iLO 2. Se non è già stata fornita, la password viene richiesta. <String> è costituito da una serie di caratteri.
- -s SocketNumber = <Integer>: numero di socket per la connessione a iLO 2. Il parametro SocketNumber deve corrispondere all'impostazione della porta dati seriale Raw sul dispositivo iLO 2 al quale si sta effettuando la connessione. Il numero di socket predefinito è 3002. <Integer> corrisponde a un numero con segno.
- -t = <Boolean>: utilizza indirettamente una connessione telnet tramite questa utility del debugger. L'impostazione predefinita prevede l'utilizzo di una connessione socket al socket numero 3002.
- -u Username = <String>: imposta il nome utente per l'accesso a iLO 2. Se non è già stato fornito, il numero utente viene richiesto. <String> è costituito da una serie di caratteri. I parametri opzionali possono essere inseriti in qualsiasi ordine.

Esempi di righe di comando:

- Per effettuare la connessione a iLO 2 mediante l'indirizzo IP 16.100.226.57, convalidare l'utente con il nome utente admin e la password mypass e avviare WinDBG.exe con la seguente riga di comando aggiuntiva:

  ```
  wilodbg 16.100.226.57 -c "-b" -u admin -p mypass
  ```

  In questo caso viene avviato WinDBG.exe con la riga di comando aggiuntiva -b e viene utilizzata una connessione socket diretta da WinDBG.exe a iLO 2 sulla porta 3002.

- Per effettuare la connessione a iLO 2 mediante l'indirizzo IP 16.100.226.57 e convalidare l'utente iLO 2 con il nome utente admin e la password mypass, e avviare kd con la riga di comando aggiuntiva -b:

  ```
  wilodbg 16.100.226.57 -k -c "-b" -u admin -p mypass -s 7734
  ```

  In questo caso viene avviato kd con la riga di comando aggiuntiva -b e viene utilizzata una connessione socket diretta da kd a iLO 2 sulla porta 7734. Per utilizzare questo esempio, è necessario configurare iLO 2 in modo da utilizzare la porta 7734.

- Per effettuare la connessione a iLO 2 mediante l'indirizzo IP 16.100.226.57 e richiedere un nome utente e una password:

  ```
  wilodbg 16.100.226.57 -c "-b" -t -e
  ```

  In questo caso viene avviato WinDBG.exe con la riga di comando aggiuntiva -b, viene utilizzata una connessione telnet crittografata da WiLODbg a iLO 2 e vengono trasmessi i dati di WinDBG.exe alla connessione telnet crittografata mediante questa utility.

Virtual Media

Virtual Media è una funzione che richiede l'utilizzo di una licenza. Se non si dispone di tale licenza, verrà visualizzato il messaggio `iLO 2 feature not licensed` (Funzione iLO 2 non concessa in licenza). Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20). La possibilità di utilizzare iLO 2 Virtual Media viene concessa o limitata attraverso privilegi utente di iLO 2. Per selezionare un supporto virtuale e connetterlo al server host, è necessario disporre del privilegio Virtual Media.

L'opzione Virtual Media (Supporti virtuali) di iLO 2 consente di disporre di un'unità dischetto e un'unità CD/DVD-ROM virtuali per avviare un server host remoto e utilizzare i supporti standard da qualsiasi punto della rete. I dispositivi Virtual Media (Supporti virtuali) sono disponibili quando il sistema host è in fase di avvio e si connettono al server host tramite la tecnologia USB. L'uso della tecnologia USB conferisce nuove funzionalità ai dispositivi di supporto virtuale di iLO 2 se i sistemi operativi supportano tale tecnologia. Sistemi operativi diversi forniscono livelli diversi di supporto USB.

- Se la funzione Virtual Floppy (Dischetto virtuale) è abilitata, in generale l'unità dischetto non è accessibile dal sistema operativo client.
- Se la funzione Virtual CD/DVD-ROM (CD/DVD-ROM virtuale) è abilitata, l'unità CD/DVD-ROM non sarà accessibile dal sistema operativo client.

△ **ATTENZIONE:** Per impedire il danneggiamento dei file e dei dati, non accedere ai supporti locali quando vengono utilizzati come supporti virtuali.

È possibile accedere ai supporti virtuali su un server host da un client tramite un'interfaccia grafica utilizzando un'applet Java™ e tramite un'interfaccia di scripting utilizzando un motore XML. L'applet Virtual Media non incorre in alcun timeout quando un dispositivo virtuale è collegato al server host. L'applet viene chiusa quando l'utente si scollega.

Per accedere ai dispositivi di supporto virtuale di iLO 2 tramite l'interfaccia basata su browser, fare clic su **Virtual Media>Virtual Media Applet** (Supporti virtuali>Applet supporti virtuali). Un'applet carica il supporto dell'unità dischetto o dell'unità CD/DVD-ROM virtuale.

È anche possibile accedere all'opzione Virtual Media (Supporti virtuali) tramite la console remota integrata, che consente di accedere alle opzioni KVM del sistema e gestire l'accensione e i supporti virtuali da un'unica console in Microsoft® Internet Explorer. Per ulteriori informazioni sull'accesso alle funzioni Virtual Power e Virtual Media mediante la console remota integrata, vedere la sezione "Opzione Integrated Remote Console" (Console remota integrata a pagina 92).

Uso dei dispositivi di supporto virtuale di iLO 2

È possibile accedere ai supporti virtuali su un server host da un client tramite un'interfaccia utilizzando un'applet Java™ e tramite un'interfaccia di scripting utilizzando un motore XML.

Per accedere ai dispositivi di supporto virtuale di iLO 2 tramite l'interfaccia grafica, nella scheda Virtual Devices (Dispositivi virtuali) selezionare l'opzione **Virtual Media** (Supporti virtuali). Un'applet carica il supporto dell'unità dischetto o dell'unità CD/DVD-ROM virtuale.

Virtual Media e Windows 7

Per impostazione predefinita, Windows 7 disattiva l'hub virtuale ILO quando all'avvio non sono abilitati o collegati dispositivi Virtual Media. Per prevenire questo problema, escludere manualmente la funzione di gestione dell'alimentazione in Windows 7 tramite il Pannello di controllo in modo che l'hub virtuale non venga disattivato.

1. Scegliere **Gestione periferiche**.
2. Fare clic su **Vista**.

3. Dal menu, selezionare **Dispositivi per connessione**.
4. Selezionare ed espandere **Controller Standard Universal Host da PCI a USB** per visualizzare i dispositivi USB incluso l'Hub USB generico che è il controller hub USB virtuale di ILO 2.
5. Fare clic con il pulsante destro del mouse su **Hub USB generico** e selezionare **Proprietà**.
6. Selezionare la scheda **Risparmio energia**.
7. Deselezionare la casella di controllo **Consenti al computer di spegnere il dispositivo per risparmiare energia**.

Floppy/chiave USB virtuale di iLO 2

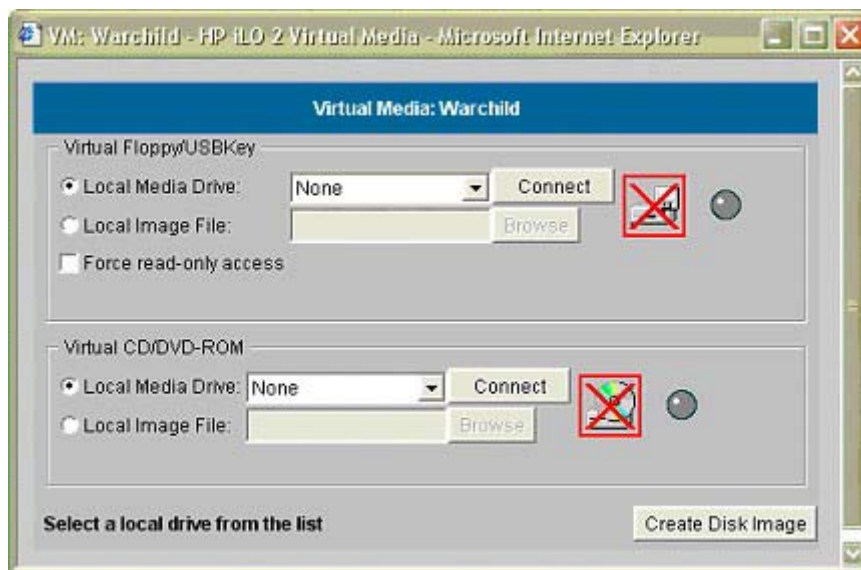
Il floppy virtuale di iLO 2 è disponibile all'avvio del server per tutti i sistemi operativi. L'avvio dal floppy virtuale di iLO 2 consente l'aggiornamento della ROM del sistema host, la distribuzione di un sistema operativo da unità di rete e il ripristino di emergenza dei sistemi operativi danneggiati.

Se il sistema operativo del server host supporta dispositivi di memorizzazione di massa USB o dispositivi Secure Digital, il floppy o la chiave USB virtuale di iLO 2 sono disponibili anche dopo il caricamento di tale sistema operativo. È possibile utilizzare il floppy o la chiave USB virtuale di iLO 2 quando il sistema operativo del server host aggiorna i driver, crea un dischetto di emergenza o esegue altre attività. Se è necessario diagnosticare e risolvere eventuali problemi con i driver del controller dell'interfaccia di rete, disporre del floppy virtuale durante l'esecuzione del server può risultare particolarmente utile.

L'unità dischetto e la chiave USB virtuale possono essere l'unità dischetto, la chiave USB o il dispositivo Secure Digital utilizzati per l'esecuzione del browser Web oppure un file di immagine memorizzato nel disco rigido o nell'unità di rete. Per ottenere le migliori prestazioni, HP consiglia di utilizzare i file di immagine locali memorizzati sull'unità disco rigido del PC client o su un'unità di rete accessibile attraverso un collegamento di rete ad alta velocità.

Per utilizzare un floppy o una chiave USB fisica sul PC client:

1. Selezionare **Local Media Drive** (Periferica locale) nella sezione Virtual Floppy/USBKey (Floppy/chiave USB virtuale).
2. Selezionare la lettera dell'unità dischetto o della chiave USB locale desiderata sul PC client dal relativo menu a discesa. Per accertarsi che il dischetto o il file di immagine di origine non venga modificato durante l'uso, selezionare l'opzione **Force read-only access** (Imponi accesso in sola lettura).
3. Fare clic su **Connect** (Connetti).

Lo stato dell'icona dell'unità connessa e del LED cambierà per indicare lo stato corrente dell'unità floppy virtuale.

Per utilizzare un file di immagine:

1. Nella sezione Virtual Floppy/USBKey (Floppy/chiave USB virtuale) dell'applet Virtual Media selezionare **Local Image File** (File di immagine locale).
2. Immettere il percorso o il nome file dell'immagine nella casella di testo oppure fare clic su **Browse** (Sfoglia) per individuare il file di immagine mediante la finestra di dialogo Choose Disk Image File (Scegli file di immagine disco). Per accertarsi che il dischetto o il file di immagine di origine non venga modificato durante l'uso, selezionare l'opzione **Force read-only access** (Imponi accesso in sola lettura).
3. Fare clic su **Connect** (Connetti).

Lo stato dell'icona dell'unità connessa e del LED cambierà per indicare lo stato corrente dell'unità floppy virtuale, dell'unità USB o del dispositivo Secure Digital. Dopo aver stabilito il collegamento, i dispositivi saranno disponibili per il server host fino alla chiusura dell'applet Virtual Media. Al termine, è possibile disconnettere il dispositivo dal server host oppure chiudere l'applet.

NOTA: Finché si utilizza un dispositivo virtuale, l'applet Virtual Media dovrà rimanere aperta sul browser.

Se il sistema operativo sul server host supporta le unità dischetto o chiave USB, l'unità dischetto/chiave USB virtuale di iLO 2 è disponibile per il server host in fase di esecuzione. Per informazioni sui sistemi operativi che supportano la memorizzazione di massa USB al momento della pubblicazione di questa guida, vedere "Supporto USB del sistema operativo" (Supporto USB del sistema operativo a pagina 117).

L'unità dischetto e la chiave USB virtuale di iLO 2 vengono visualizzate nel sistema operativo esattamente come una qualsiasi altra unità. Quando si usa iLO 2 per la prima volta, può essere necessario completare una procedura guidata di installazione del nuovo hardware.

Dopo aver terminato di utilizzare il supporto virtuale iLO 2 e averlo scollegato, potrebbe comparire un messaggio di avviso relativo alla rimozione non sicura di un dispositivo. Per evitare la visualizzazione di tale messaggio, ricorrere alla funzione inclusa nel sistema operativo per arrestare il dispositivo prima di scollegarlo dal supporto virtuale.

Note sui sistemi operativi con l'utilizzo di un'unità dischetto/chiave USB virtuale

- MS-DOS

  Durante l'avvio e l'esecuzione di una sessione MS-DOS, l'unità dischetto virtuale viene visualizzata come un'unità dischetto standard del BIOS. Viene quindi visualizzata come unità A. Se è presente anche un'unità dischetto fisica, questa non viene visualizzata e risulta pertanto non disponibile. Non è possibile utilizzare simultaneamente un'unità dischetto locale fisica e un'unità dischetto virtuale.

- Windows Server® 2008 o versioni successive e Windows Server® 2003

  Le unità dischetto e chiave USB virtuali vengono automaticamente visualizzate non appena Microsoft® Windows® riconosce il dispositivo USB collegato. Utilizzare le unità esattamente come se si trattasse di dispositivi collegati localmente.

  Per utilizzare un'unità dischetto virtuale come dischetto dei driver durante un'installazione di Windows®, disabilitare l'unità dischetto integrata nell'host RBSU che determina la visualizzazione dell'unità dischetto virtuale come unità A.

  Per utilizzare la chiave USB virtuale come dischetto dei driver durante un'installazione di Windows®, modificare l'ordine di avvio della chiave USB nell'utility RBSU del sistema. HP consiglia di posizionare l'unità chiave USB al primo posto dell'ordine di avvio.

- Windows Vista®

  Se si utilizza Internet Explorer 7 con la modalità protetta attiva, Windows Vista® non supporta correttamente i supporti virtuali. Vengono infatti visualizzati vari messaggi di errore, ad esempio `could not open cdrom (the parameter is incorrect)` (impossibile aprire cdrom (parametro non corretto)). Per utilizzare i supporti virtuali, fare clic su **Strumenti/Opzioni Internet/ Protezione**, disattivare l'opzione **Attiva modalità protetta**, quindi scegliere **Applica**. Dopo aver disabilitato la modalità protetta, chiudere tutte le istanze aperte del browser e riavviarlo.

- NetWare 6.5

  NetWare 6.5 supporta l'uso delle unità dischetto e chiave USB. Istruzioni dettagliate sono riportate nella sezione "Attivazione di un'unità dischetto/chiave USB virtuale con NetWare 6.5" (Attivazione di un'unità dischetto/chiave USB virtuale con NetWare 6.5 a pagina 118).

- Red Hat e SUSE Linux

  Linux supporta l'uso delle unità dischetto e chiave USB. Istruzioni dettagliate sono riportate nella sezione "Attivazione di un'unità dischetto/chiave USB virtuale in Linux" (Attivazione di un'unità dischetto/chiave USB virtuale in Linux a pagina 118).

Supporto USB del sistema operativo

Per utilizzare i supporti virtuali è necessario che il sistema operativo utilizzato supporti i dispositivi USB e i dispositivi storage USB. Attualmente, i dispositivi USB sono supportati in Windows Server® 2008, Windows® 2003, Red Hat Enterprise Linux 3, Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, SUSE SLES 9,e SUSE SLES 10. I dispositivi storage USB sono tuttavia supportati anche da altri sistemi operativi.

Durante l'avvio del sistema, il BIOS della ROM fornisce il supporto USB fino al caricamento del sistema operativo. Dal momento che l'ambiente MS-DOS utilizza il BIOS per comunicare con i dispositivi storage, i dischetti dell'utility per l'avvio DOS funzionano anche con i supporti virtuali.

NOTA: RedHat Enterprise Linux 3 non consente di avvalersi di un dischetto dei driver durante l'utilizzo di supporti virtuali.

Attivazione di un'unità dischetto/chiave USB virtuale con NetWare 6.5

1. Accedere a iLO 2 tramite un browser.
2. Nella scheda Virtual Devices (Dispositivi virtuali) fare clic su **Virtual Media** (Supporti virtuali).
3. Inserire il supporto nell'unità dischetto locale, selezionare un'unità dischetto e scegliere **Connect** (Connetti). In alternativa, selezionare l'immagine del dischetto da utilizzare e scegliere **Connect** (Connetti).

In NetWare 6.5, utilizzare il comando `lfvmount` sulla console del server per assegnare una lettera di unità al dispositivo.

Il sistema operativo NetWare 6.5 assegnerà la prima lettera di unità disponibile all'unità dischetto virtuale. È ora possibile utilizzare il comando `volumes` dalla console del server per visualizzare lo stato del nuovo dispositivo.

Quando la lettera di unità appare come montata, l'unità sarà disponibile per l'accesso dall'interfaccia grafica utente del server e dalla console di sistema.

Quando l'unità dischetto virtuale è montata, se il supporto nell'unità dischetto locale viene modificato, sarà necessario eseguire nuovamente il comando `lfvmount` sulla console del server affinché il sistema operativo NetWare 6.5 visualizzi correttamente il nuovo supporto.

Attivazione di un'unità dischetto/chiave USB virtuale in Linux

1. Accedere a iLO 2 tramite un browser.
2. Nella scheda Virtual Devices (Dispositivi virtuali) fare clic su **Virtual Media** (Supporti virtuali).
3. Selezionare un'unità dischetto o un'immagine del dischetto.

   a. Per un'unità dischetto o un'immagine selezionare una periferica locale o un file di immagine locale e fare clic su **Connect** (Connetti).

   b. Per un'unità chiave USB o un'immagine selezionare un file di immagine locale e fare clic su **Connect** (Connetti).

   Per un'unità chiave USB fisica immettere `/dev/sda` nella casella di testo Local Image File (File di immagine locale).

4. Caricare i driver USB utilizzando i seguenti comandi:

```
modprobe usbcore
modprobe usb-storage
modprobe usb-ohci
```

5. Caricare il driver per l'unità disco SCSI utilizzando il seguente comando:

```
modprobe sd_mod
```

6. Montare l'unità.

   - Per montare l'unità dischetto, utilizzare il seguente comando:

```
mount /dev/sda /mnt/floppy -t vfat
```

   - Per montare l'unità chiave USB, utilizzare il seguente comando:

```
mount /dev/sda1 /mnt/keydrive
```

NOTA: Utilizzare il comando `man mount` per ottenere informazioni sugli altri tipi di file system.

È possibile utilizzare l'unità dischetto e la chiave USB come un file system Linux, se formattate in tal modo, utilizzando il comando `mount`. L'accesso ai dischetti da 1,44 MB viene tuttavia di norma effettuato mediante le utility mtools distribuite con i sistemi operativi Red Hat e SLES. La configurazione mtools predefinita non riconosce un'unità dischetto collegata mediante USB. Per abilitare i diversi comandi m che consentono di accedere al dispositivo dischetto virtuale, modificare il file /etc/mtools.conf esistente e aggiungere la seguente riga:

```
drive v: file="/dev/sda" exclusive
```

Per abilitare i diversi comandi mtools che consentono di accedere al dispositivo chiave USB virtuale, modificare il file /etc/mtools.conf esistente e aggiungere la seguente riga:

```
drive v: file="/dev/sda1" exclusive
```

Per visualizzare la tabella delle partizioni del dispositivo chiave USB virtuale allo scopo di individuare la partizione desiderata, utilizzare il seguente comando:

```
fdisk -l /dev/sda
```

Questa modifica permette alla suite mtools di accedere al dischetto virtuale come unità v. Ad esempio:

```
mcopy /tmp/XXX.dat v:
mdir v:
mcopy v:foo.dat /tmp/XXX
```

Cambio di dischetti

Quando si utilizzano unità dischetto o unità chiave USB virtuali iLO 2 e l'unità dischetto fisica del client è un'unità dischetto USB, le operazioni di cambio del disco non verranno riconosciute. Ad esempio, in questa configurazione, se si ottiene una visualizzazione di directory da un dischetto e si cambia il dischetto, nella successiva visualizzazione di directory verrà mostrato l'elenco del primo dischetto. Se è necessario cambiare disco quando si utilizza il dischetto o la chiave USB virtuali iLO 2, verificare che il client contenga un'unità dischetto non USB.

Unità CD/DVD-ROM virtuale di iLO 2

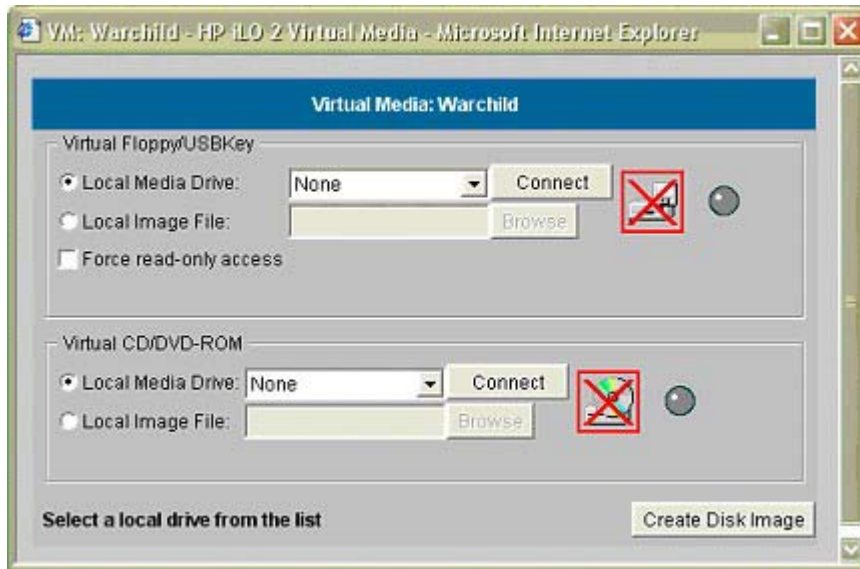
L'unità CD/DVD-ROM virtuale di iLO 2 è disponibile all'avvio del server per i sistemi operativi specificati nella sezione "Supporto USB del sistema operativo" (Supporto USB del sistema operativo a pagina 117). L'avvio dall'unità CD/DVD-ROM virtuale di iLO 2 consente ad esempio di installare un sistema operativo da unità di rete e di eseguire il recupero di emergenza di sistemi operativi danneggiati.

Se il sistema operativo del server host supporta dispositivi di memorizzazione di massa USB, l'unità CD/DVD-ROM virtuale di iLO 2 è disponibile anche dopo il caricamento di tale sistema operativo. È possibile utilizzare l'unità CD/DVD-ROM virtuale di iLO 2 quando il sistema operativo del server host aggiorna i driver dei dispositivi, installa il software o esegue altre operazioni. Se è necessario diagnosticare e risolvere eventuali problemi con i driver del controller dell'interfaccia di rete, disporre del CD/DVD-ROM virtuale durante l'esecuzione del server può risultare particolarmente utile.

L'unità CD/DVD-ROM virtuale può essere l'unità fisica del computer utilizzata per l'esecuzione del browser Web oppure un file di immagine memorizzato nel disco rigido o nell'unità di rete.

NOTA: Per ottimizzare le prestazioni utilizzare i file di immagine. HP consiglia di utilizzare i file di immagine locali memorizzati sull'unità disco rigido del PC client o su un'unità di rete accessibile attraverso un collegamento di rete ad alta velocità.

Per utilizzare un'unità CD/DVD-ROM fisica sul PC client:

1. Selezionare **Local Media Drive** (Periferica locale) nella sezione Virtual CD/DVD-ROM (CD/DVD-ROM virtuale).
2. Selezionare la lettera dell'unità CD/DVD-ROM fisica desiderata sul PC client dal relativo menu a discesa.
3. Fare clic su **Connect** (Connetti).

Per utilizzare un file di immagine:

1. Nella sezione Virtual CD/DVD-ROM (Unità CD/DVD-ROM virtuale) dell'applet Virtual Media selezionare **Local Image File** (File di immagine locale).
2. Immettere il percorso o il nome file dell'immagine nella casella di testo oppure fare clic su **Browse** (Sfoglia) per individuare il file di immagine mediante la finestra di dialogo Choose Disk Image File (Scegli file di immagine disco).
3. Fare clic su **Connect** (Connetti).

Lo stato dell'icona dell'unità connessa e del LED cambierà per indicare lo stato corrente dell'unità CD/DVD-ROM virtuale. Dopo aver stabilito il collegamento, i dispositivi virtuali sono disponibili al server host fino alla chiusura dell'applet Virtual Media. Per smettere di utilizzare il CD/DVD-ROM virtuale, disconnettere il dispositivo dal server host oppure chiudere l'applet. Quando si utilizza un dispositivo di supporto virtuale, l'applet Virtual Media deve rimanere aperta.

Se il sistema operativo sul server host supporta le unità dischetto USB, allora l'unità CD/DVD-ROM virtuale di iLO 2 sarà disponibile per il server host durante l'esecuzione. Per informazioni sui sistemi operativi che supportano la memorizzazione di massa USB al momento della pubblicazione di questa guida, vedere "Supporto USB del sistema operativo" (Supporto USB del sistema operativo a pagina 117).

L'unità CD/DVD-ROM virtuale di iLO 2 viene visualizzata nel sistema operativo esattamente come qualsiasi altra unità CD/DVD-ROM. Quando si usa iLO 2 per la prima volta, può essere necessario completare una procedura guidata di installazione del nuovo hardware.

Dopo aver terminato di utilizzare il supporto virtuale iLO 2 e averlo scollegato, potrebbe comparire un messaggio di avviso relativo alla rimozione non sicura di un dispositivo. Per evitare la visualizzazione

di tale messaggio, ricorrere alla funzione inclusa nel sistema operativo per arrestare il dispositivo prima di scollegarlo dal supporto virtuale.

Note sui sistemi operativi con l'utilizzo di CD/DVD-ROM virtuale

- MS-DOS

  L'unità CD/DVD-ROM virtuale non è supportata dal sistema operativo MS-DOS.

- Windows Server® 2008 e Windows Server® 2003

  L'unità CD/DVD-ROM virtuale viene visualizzata automaticamente dopo che Windows® ha riconosciuto l'attivazione del dispositivo USB. Utilizzare l'unità CD/DVD-ROM virtuale esattamente come un dispositivo collegato localmente.

- Linux
  - Red Hat Linux

    Sui server provvisti di un'unità CD/DVD-ROM IDE collegata localmente, è possibile accedere al dispositivo CD/DVD-ROM virtuale tramite il comando /dev/cdrom1. Sui server sprovvisti di unità CD/DVD-ROM collegate localmente, quali i sistemi blade BL-class, l'unità CD/DVD-ROM virtuale è la prima unità CD/DVD-ROM accessibile tramite il comando /dev/cdrom.

    L'unità CD/DVD-ROM virtuale può essere attivata come un normale dispositivo CD/DVD-ROM tramite il comando:

    mount /mnt/cdrom1

  - SLES 9

    Il sistema operativo SLES 9 imposta una posizione diversa per le unità CD/DVD-ROM collegate tramite l'interfaccia USB. L'unità CD/DVD-ROM virtuale può quindi essere individuata nella posizione /dev/scd0, a meno che non sia presente un'unità CD/DVD-ROM locale collegata tramite l'interfaccia USB. In tal caso, la posizione sarà /dev/scd1.

    L'unità CD/DVD-ROM virtuale può essere attivata come un normale dispositivo CD/DVD-ROM tramite il comando:

    mount /dev/scd0 /media/cdrom11

    Le istruzioni dettagliate sono riportate nella sezione "Installazione del CD-ROM Virtual Media in Linux" (Installazione del CD/DVD-ROM Virtual Media in Linux a pagina 121).

Installazione del CD/DVD-ROM Virtual Media in Linux

1. Accedere a iLO 2 tramite un browser.
2. Nella scheda Virtual Devices (Dispositivi virtuali) fare clic su **Virtual Media** (Supporti virtuali).
3. Selezionare l'unità CD/DVD-ROM da utilizzare e fare clic su **Connect** (Connetti).
4. Montare l'unità mediante il seguente comando:

   ```
   mount /dev/cdrom1 /mnt/cdrom1
   ```

   Per SLES 9:

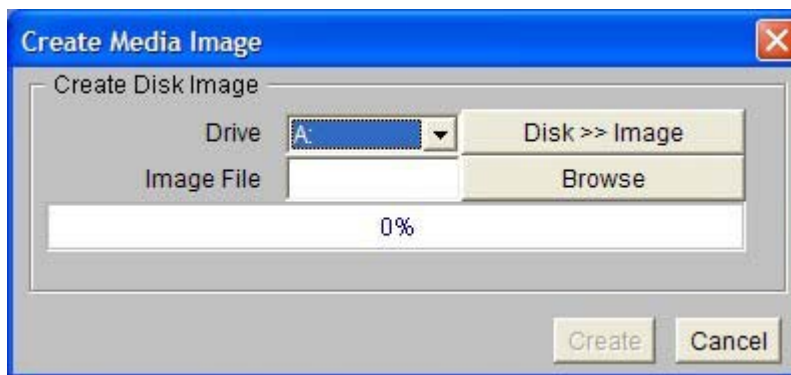
   ```
   mount /dev/scd0 /media/cdrom1
   ```

Creazione di file di immagine disco iLO 2

La funzione Virtual Media (Supporti virtuali) di iLO 2 consente di creare file di immagine dell'unità dischetto e dell'unità CD-ROM nella stessa applet. La creazione di file di immagine dell'unità DVD

mediante l'applet Virtual Media (Supporti virtuali) non è supportata. I file di immagine creati dall'applet sono immagini di file system ISO-9660. Quando si usano i file di immagine, le prestazioni del supporto virtuale di iLO 2 sono superiori. La utility che consente di creare file di immagine del dischetto e del disco CD-ROM virtuale iLO 2 è integrata nell'applet Virtual Media (Supporti virtuali). È tuttavia possibile creare immagini anche tramite strumenti standard come DD.

Per creare un file di immagine:

1. Fare clic su **Create Disk Image** (Crea immagine disco).
2. Selezionare l'unità del supporto locale dal menu a discesa.
3. Immettere il percorso o il nome file nella casella di testo oppure fare clic su **Browse** (Sfoglia) per selezionare un file di immagine esistente o per modificare la directory in cui verrà creato il file di immagine.
4. Fare clic su **Create** (Crea). L'applet Virtual Media avvia il processo di creazione del file di immagine. Il processo termina quando la barra di avanzamento raggiunge il 100%. Per annullare il processo di creazione di un file di immagine, fare clic su **Cancel** (Annulla).

L'opzione Disk>>Image (Disco>>Immagine) consente di creare file di immagine da dischetti o CD-ROM fisici. L'opzione Image>>Disk (Immagine>>Disco) non è valida per un'immagine CD-ROM virtuale. Quando si fa clic, il pulsante Disk>>Image (Disco>>Immagine) diventa Image>>Disk (Immagine>>Disco). Fare clic su questo pulsante per passare dalla creazione di file di immagine da dischetti fisici alla creazione di dischetti fisici da file di immagine.

Cartella virtuale

La cartella virtuale di iLO 2 emula un dispositivo USB, creando dinamicamente un'immagine virtuale di una cartella o directory selezionata. Dopo aver creato un'immagine virtuale di una cartella o directory, il server esegue la connessione all'immagine creata come un dispositivo storage USB, consentendo così di accedere al server e trasferire i file dall'immagine generata da iLO 2 a una posizione qualsiasi del server.

La funzionalità Virtual Folder (Cartella virtuale) è disponibile soltanto nella console remota integrata. La cartella virtuale non è un dispositivo di avvio, è di sola lettura e la cartella attivata è statica. Le modifiche apportate al file del client non vengono replicate nella cartella attivata.

La funzionalità Virtual Folder (Cartella virtuale) richiede l'utilizzo di una licenza e può essere acquistata insieme a iLO 2 Advanced o iLO 2 Select. Mediante questa funzionalità è possibile selezionare e trasferire file da un client a un server gestito. Questa funzionalità consente inoltre di attivare e disattivare una directory in una directory locale o connessa in rete accessibile attraverso il client, attivata e disattivata come un dispositivo Virtual Media.

Note sul sistema operativo della cartella virtuale

- MS-DOS

  Durante l'avvio e le sessioni MS-DOS, il dispositivo della cartella virtuale viene visualizzato come un'unità dischetto standard del BIOS. Il dispositivo viene visualizzato come unità A. Se è presente anche un'unità dischetto fisica, questa non viene visualizzata e risulta pertanto non disponibile. Non è possibile utilizzare simultaneamente un'unità dischetto locale fisica e la cartella virtuale.

- Windows®

  Il dispositivo della cartella virtuale viene visualizzato automaticamente non appena Microsoft® Windows® riconosce l'attivazione del dispositivo USB virtuale. La cartella virtuale può essere utilizzata come un normale dispositivo collegato localmente. La cartella virtuale non è un dispositivo di avvio. Se si tenta di eseguire l'avvio dalla cartella, è possibile che il server non possa essere avviato.

- NetWare 6.5

  NetWare 6.5 supporta l'utilizzo della cartella virtuale come unità dischetto e unità chiave USB. Istruzioni dettagliate sono riportate nella sezione "Attivazione di un'unità dischetto/chiave USB virtuale con NetWare 6.5" (Attivazione di un'unità dischetto/chiave USB virtuale con NetWare 6.5 a pagina 118).

- Red Hat e SLES Linux

  Linux supporta l'utilizzo della cartella virtuale. La cartella virtuale utilizza un formato file system FAT 16. Per ulteriori informazioni, vedere la sezione "Attivazione di un supporto/unità chiave virtuale USB in Linux" (Attivazione di un'unità dischetto/chiave USB virtuale in Linux a pagina 118).

Gestione dell'alimentazione

Il software di gestione dell'alimentazione di iLO 2 consente di visualizzare e controllare lo stato di alimentazione del server, monitorare l'utilizzo dell'alimentazione, monitorare il processore e modificare le impostazioni di alimentazione. Nella pagina Power Management (Gestione alimentazione) sono disponibili quattro opzioni di menu: Server Power (Alimentazione server), Power Meter (Contatore alimentazione), Processor States (Stati processore) e Settings (Impostazioni). Quando si seleziona **Power Management** (Gestione dell'alimentazione) viene visualizzata la pagina Server Power Controls (Controlli alimentazione server). La pagina Server Power Controls (Controlli alimentazione server) è divisa in due sezioni: Virtual Power Button (Pulsante di accensione virtuale) e Power Configuration Settings (Impostazioni configurazione alimentazione).

Nella sezione Virtual Power Button (Pulsante di accensione virtuale) viene visualizzato lo stato di alimentazione corrente del server nonché le opzioni di controllo dell'alimentazione del server remoto. Lo stato di alimentazione visualizzato è lo stato di alimentazione del server nel momento in cui è stata aperta la pagina. Lo stato del server può essere On (Acceso), Off (Spento) o Reset (Reimpostazione). Utilizzare la funzione di aggiornamento del browser per mantenere aggiornato lo stato dell'indicatore di alimentazione.

Per modificare lo stato di alimentazione corrente del server utilizzando le opzioni della sezione Virtual Power Button (Pulsante di accensione virtuale), è necessario disporre dei privilegi di accensione virtuale e di ripristino. Alcune delle opzioni di controllo dell'alimentazione non consentono di eseguire il normale arresto del sistema operativo ovvero di effettuare la chiusura tramite la console remota prima di utilizzare le opzioni della sezione Virtual Power Button (Pulsante di accensione virtuale). Sono disponibili le opzioni riportate di seguito:

- Il pulsante Momentary Press (Pressione momentanea) consente di eseguire le stesse operazioni che vengono eseguite premendo il pulsante di alimentazione fisico.
- L'utilizzo dell'opzione Press and Hold (Pressione mantenuta) equivale a premere il pulsante di alimentazione fisico per cinque secondi e quindi rilasciarlo. Questa opzione fornisce la funzionalità di compatibilità ACPI implementata da alcuni sistemi operativi. Questi sistemi operativi presentano comportamenti diversi a seconda che venga esercitata una pressione breve o lunga. Il comportamento di questa opzione può compromettere le normali funzioni di arresto del sistema operativo.
- L'avvio a freddo del sistema rimuove immediatamente l'alimentazione dal sistema. e si riavvierà dopo circa sei secondi. Questa opzione non è disponibile quando il server è spento. e compromette le normali funzioni di arresto del sistema operativo.
- L'opzione Reset System (Reimposta sistema) avvia un ripristino del sistema. Questa opzione non è disponibile quando il server è spento. Il comportamento di questa opzione può compromettere le normali funzioni di arresto del sistema operativo.

La sezione Power Configuration Settings (Impostazioni configurazione alimentazione) consente di controllare la modalità di accensione del server remoto quando viene applicata l'alimentazione. Sono disponibili le opzioni riportate di seguito:

- Automatically Power On Server (Accendi server automaticamente) consente a iLO 2 di accendere un server quando viene fornita corrente, ad esempio quando il server viene collegato alla rete elettrica o quando un gruppo di continuità si attiva in seguito all'interruzione dell'alimentazione. Per modificare questa impostazione è necessario disporre dei privilegi Virtual Power (Accensione virtuale) e Reset (Reimpostazione).

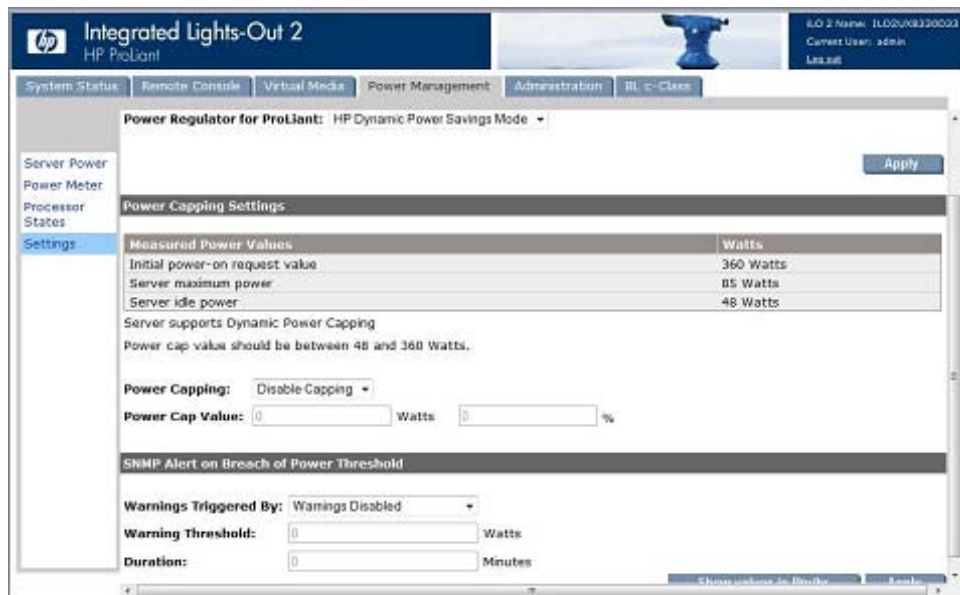
  La mancanza imprevista di alimentazione durante l'accensione del server comporta la riaccensione del server, indipendentemente dall'impostazione di accensione automatica.

- L'opzione Power On Delay (Ritardo accensione) viene utilizzata per scaglionare l'accensione dei server all'interno di un datacenter. I server blade sono controllati dall'infrastruttura rack e non supportano un ritardo di accensione. L'opzione Power On Delay (Ritardo accensione) non interferisce con il pulsante di accensione.

  Il ritardo di accensione si verifica prima che il server venga acceso da iLO 2, inclusa l'accensione automatica e il ripristino dell'alimentazione. In alcuni server non è possibile applicare il ritardo di accensione nel caso di ripristino dell'alimentazione. Il firmware di iLO 2 richiede circa 10 secondi prima che possa essere effettuata l'accensione del server. Per modificare questa impostazione è necessario disporre dei privilegi Virtual Power (Accensione virtuale) e Reset (Reimpostazione).

Impostazioni di alimentazione del server

La funzione Power Regulator for ProLiant (Regolatore di alimentazione per ProLiant) consente a iLO 2 di modificare dinamicamente i livelli di frequenza e voltaggio dei processori sulla base delle condizioni operative per garantire un risparmio energetico con effetti minimi sulle prestazioni. I processori che supportano questa funzione sono impostati su stati predefiniti di voltaggio e frequenza, detti *p-states* (stati p). Il software consente di passare il processore dinamicamente da uno stato p ad un altro. P-0 è la combinazione di frequenza e voltaggio più alta supportata dal processore. La modifica dello stato p del processore in base all'utilizzo della CPU consente di ottenere un significativo risparmio energetico senza influire sulle prestazioni, riducendo il voltaggio e la frequenza dei processori quando il sistema non è attivo e aumentandoli quando necessario.

Nella pagina Power Management Settings (Impostazioni di gestione dell'alimentazione) è possibile visualizzare e controllare la modalità di regolazione dell'alimentazione del server. Solo gli utenti che dispongono del privilegio Configure iLO Settings (Configura impostazioni di iLO) possono modificare questa impostazione.

- La sezione Power Regulator for ProLiant (Regolatore di alimentazione per ProLiant) comprende le seguenti opzioni:
  - Enable HP Dynamic Power Savings Mode (Abilita modalità dinamica risparmio energetico HP) consente di impostare dinamicamente il livello di potenza del processore in base all'utilizzo.
  - Enable HP Static Low Power Mode (Abilita modalità alimentazione ridotta statica HP) consente di impostare il processore su un utilizzo dell'alimentazione ridotto al minimo.
  - HP Static High Performance Mode (Modalità di massime prestazioni statiche HP) forza il processore ad operare continuamente nel massimo stato di utilizzo dell'alimentazione supportato.
  - Enable OS Control Mode (Abilita modalità di controllo da sistema operativo) consente di impostare il processore sul massimo utilizzo dell'alimentazione.

    Dopo aver selezionato una delle opzioni della sezione Power Regulator for ProLiant (Regolatore di alimentazione per ProLiant), fare clic su **Apply** (Applica) per salvare l'impostazione. Perché la modifica sia effettiva, è necessario riavviare il server. Non è possibile modificare tali impostazioni durante il POST del server. Se le impostazioni non vengono modificate dopo aver selezionato **Applica**, è possibile che il server sia in fase di avvio o debba essere riavviato. Chiudere i programmi RBSU in esecuzione, consentire il completamento della procedura POST ed eseguire nuovamente l'operazione.
- Nella sezione Power Capping Settings (Impostazioni limitazione alimentazione) è possibile visualizzare i valori di alimentazione misurati, impostare un limitatore di alimentazione e disabilitare la limitazione dell'alimentazione.

  I valori di alimentazione misurati includono il valore massimo di alimentazione del server, l'alimentazione massima del server e l'alimentazione fornita durante l'inattività del server. Il valore massimo di alimentazione del server fa riferimento alla quantità massima di energia che può essere fornita dall'alimentatore del server. I valori di alimentazione massima e alimentazione in stato di inattività vengono determinati da due test di alimentazione eseguiti dalla ROM durante il POST.

  Power Cap Setting (Impostazioni limitazione alimentazione) consente di impostare un limitatore di alimentazione sul server. Dopo che è stato impostato un limitatore di alimentazione, la lettura dell'alimentazione media del server nel tempo deve essere uguale o inferiore al valore del

limitatore. È possibile impostare il limitatore di alimentazione specificando un valore watt o Btu/hr (fare clic su **Show values in Btu/hr**, Visualizza valori in Btu/hr) o una percentuale. La percentuale fa riferimento alla differenza tra i valori di alimentazione massima e in stato di inattività del server. Il valore del limitatore non può essere impostato al di sotto del valore di alimentazione del server in stato di inattività.

Le impostazioni di Power Capping (Limitazione alimentazione) sono disabilitate quando il server fa parte di un Enclosure Dynamic Power Cap (Limite alimentazione dinamica contenitore). Questi valori possono essere impostati e modificati utilizzando Onboard Administrator o Insight Power Manager.

◦ Se il server è dotato di componenti hardware e software in grado di supportare la limitazione dell'alimentazione dinamica, viene visualizzato il messaggio `System supports Dynamic Power Capping` (Il sistema supporta la limitazione dell'alimentazione dinamica). La limitazione dell'alimentazione dinamica garantisce la protezione degli interruttori elettrici.

◦ Se il messaggio `System supports Dynamic Power Capping` (Il sistema supporta la limitazione dell'alimentazione dinamica) non viene visualizzato, il server supporta la normale limitazione dell'alimentazione, che non presenta una velocità di reazione sufficiente a fornire la protezione degli interruttori elettrici.

  Per ulteriori informazioni sulla limitazione dell'alimentazione dinamica, vedere "Limitazione dell'alimentazione dinamica per server blade".

- La sezione relativa agli avvisi SNMP in caso di superamento della soglia energetica consente di impostare l'invio di avvisi di tipo SNMP ogni volta che il consumo di energia elettrica supera un valore soglia predefinito. È possibile impostare i seguenti valori:

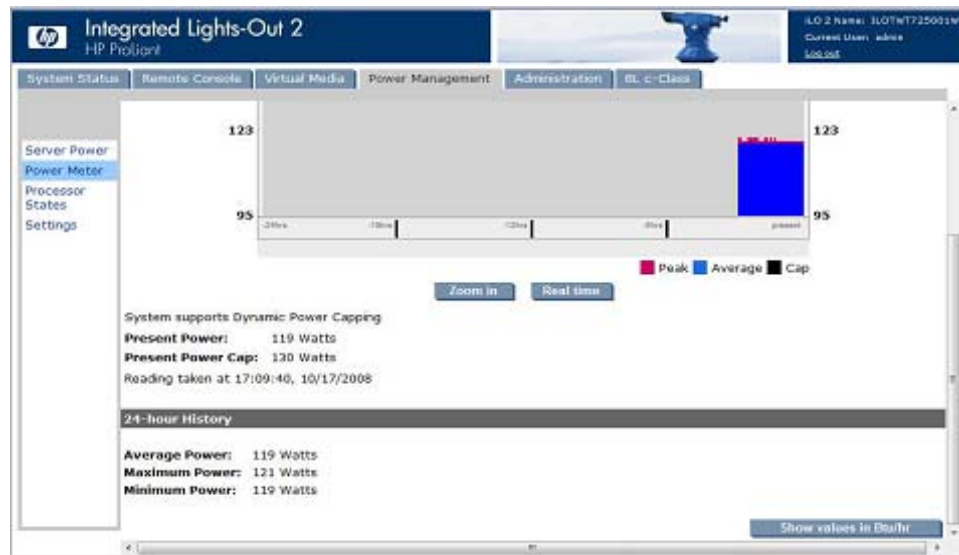
  ◦ Warnings Triggered By (Avvisi attivati da): consente di specificare se gli avvisi devono essere basati sui valori di picco o sui valori medi del consumo energetico oppure disattivati.

  ◦ Warning Threshold (Soglia avvisi): consente di impostare il valore soglia che il consumo energetico deve superare per determinare l'attivazione di un avviso SNMP.

  ◦ Duration (Durata): consente di impostare l'intervallo di tempo, espresso in minuti, che il consumo energetico deve rimanere superiore al valore soglia prima che sia attivato l'avviso SNMP. È necessario che il valore non superi 240 minuti e che sia un multiplo di 5.

Per rendere effettive le impostazioni selezionate, fare clic su **Apply** (Applica). Alcuni server consentono la modifica dei livelli di alimentazione dei processori mediante l'utility RBSU del sistema. Per ulteriori informazioni, consultare la guida utente del sistema.

Dati relativi all'alimentazione del server

iLO 2 consente di visualizzare graficamente l'utilizzo dell'alimentazione del server. Nella pagina Power Meter Readings (Letture del contatore di alimentazione) il consumo energetico del server viene visualizzato in formato grafico. Per accedere alla pagina Power Meter Readings (Letture del contatore di alimentazione), selezionare **Power Management** (Gestione alimentazione) e fare clic su **Power Meter** (Contatore di alimentazione). La pagina Power Meter Readings (Letture del contatore di alimentazione) è divisa in due sezioni: Power Meter Readings (Letture del contatore di alimentazione) e 24-Hour History (Cronologia 24 ore).

Nella sezione Power Meter Readings (Letture del contatore di alimentazione) viene visualizzato quanto segue:

- Il grafico dati illustra l'utilizzo dell'alimentazione del server durante le ultime 24 ore. iLO 2 raccoglie dal server informazioni sull'utilizzo dell'alimentazione ogni cinque minuti. Per ciascun intervallo di cinque minuti vengono memorizzati il valore di picco e il valore medio relativi all'utilizzo dell'alimentazione in un buffer circolare. Questi due valori vengono visualizzati sotto forma di grafico a barre, con i valori medi riportati in blu e quelli di picco in rosso. Questi dati vengono reimpostati ogni volta che il server o iLO 2 viene ripristinato.
  - Per aumentare la dimensione di visualizzazione del grafico, fare clic su **Zoom in** (Zoom avanti). In questo modo verrà aumentata la larghezza orizzontale delle barre di dati del grafico. In questa modalità viene visualizzato un dispositivo di scorrimento che consente di esaminare i dati all'interno della finestra.
  - Per visualizzare il consumo energetico corrente, fare clic su **Real Time** (Tempo reale). Nel grafico dati Real Time (Tempo reale) vengono visualizzate informazioni sul consumo energetico relativo agli ultimi 20 minuti, inclusi i valori di picco, i valori medi e la limitazione dell'alimentazione.
- Il supporto corrente per Dynamic Power Capping (Limitazione dell'alimentazione dinamica).

- Il valore Present Power (Alimentazione corrente) indica il valore di alimentazione correntemente misurato dal server.
- Il valore Present Power Cap (Limitatore di alimentazione presente) visualizza l'impostazione del limitatore di alimentazione corrente.

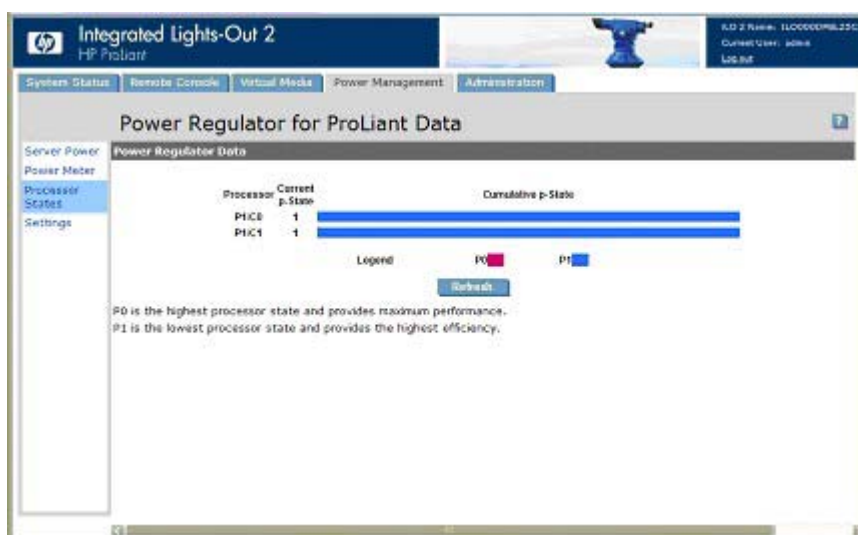
Nella sezione 24-Hour History (Cronologia 24 ore) viene visualizzato quanto segue:

- Average Power Reading (Lettura di alimentazione media) indica il valore medio di alimentazione delle misurazioni del server nelle ultime 24 ore. Se il server è in esecuzione da meno di 24 ore, il valore corrisponde alla media di tutte le misurazioni effettuate a partire dall'avvio del server.
- Maximum Power (Alimentazione massima) indica il valore massimo di alimentazione delle misurazioni del server nelle ultime 24 ore. Se il server è in esecuzione da meno di 24 ore, il valore corrisponde al valore massimo di tutte le misurazioni effettuate a partire dall'avvio del server.
- Minimum Power (Alimentazione minima) indica il valore minimo di alimentazione delle misurazioni del server nelle ultime 24 ore. Se il server è in esecuzione da meno di 24 ore, il valore corrisponde al valore minimo di tutte le misurazioni effettuate a partire dall'avvio del server.
- L'opzione Show value in BTUs (Visualizza valore in BTU) converte i dati visualizzati da watt a BTU.

Stati del processore

Nella pagina Power Regulator for ProLiant Data (Dati regolatore di alimentazione per ProLiant) è possibile visualizzare il P-state (stato p) corrente dei processori, oltre a una media mobile della percentuale di tempo trascorsa da ogni processore logico in ciascun P-state (stato p) durante le precedenti 24 ore. Per aggiornare il grafico dati P-state, fare clic su **Refresh** (Aggiorna).

Per visualizzare la pagina Power Regulator for ProLiant Data (Dati regolatore di alimentazione per ProLiant), è necessario disporre del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2). Power Regulator for ProLiant Data è una funzionalità che richiede un'apposita licenza e può essere acquistata insieme a licenze opzionali. Per ulteriori informazioni, vedere la sezione "Licenze" (Licenze a pagina 20).

Per accedere alla pagina Power Regulator for ProLiant Data (Dati regolatore di alimentazione per ProLiant), fare clic su **Power Management>Processor States** (Gestione alimentazione>Stati processore)

Nella pagina Power Regulator Data (Dati regolatore alimentazione) vengono visualizzati i dati P-state raccolti ogni secondo e quindi aggiornati per la visualizzazione ogni 5 minuti. Lo stato corrente di ciascun processore logico viene registrato dalla ROM di sistema. Lo stato registrato nelle piattaforme basate su Intel® riflette la frequenza e il voltaggio correnti. Se sono presenti più processori, è possibile che lo stato non corrisponda a un p-state (stato p) assoluto a causa delle dipendenze tra i processori. È infatti possibile che la frequenza corrisponda a un determinato p-state (stato p), mentre il voltaggio corrisponda a un p-state (stato p) superiore. La ROM di sistema aggiorna i dati del p-state (stato p) per la frequenza corrente ma non per il voltaggio corrente.

I dati vengono rappresentati mediante un grafico a barre, dove la lunghezza totale della barra corrisponde al 100% del tempo coperto dai dati stessi. Viene visualizzato un grafico dati per ciascun processore o core. I grafici dati per più thread su un processore o core con supporto per Hyper-Threading non verranno visualizzati. Il periodo di tempo trascorso dal processore in ciascun p-state (stato p) viene indicato mediante la colorazione di porzioni della barra, utilizzando un colore diverso per ciascuno stato. Le dimensioni delle porzioni colorate vengono determinate in base alla percentuale del tempo totale trascorso dal processore nel p-state (stato p) in questione. Se si posiziona il mouse sul grafico a barre, viene visualizzato un messaggio in cui è indicata la percentuale numerica rappresentata dalla porzione della barra.

Efficienza di alimentazione

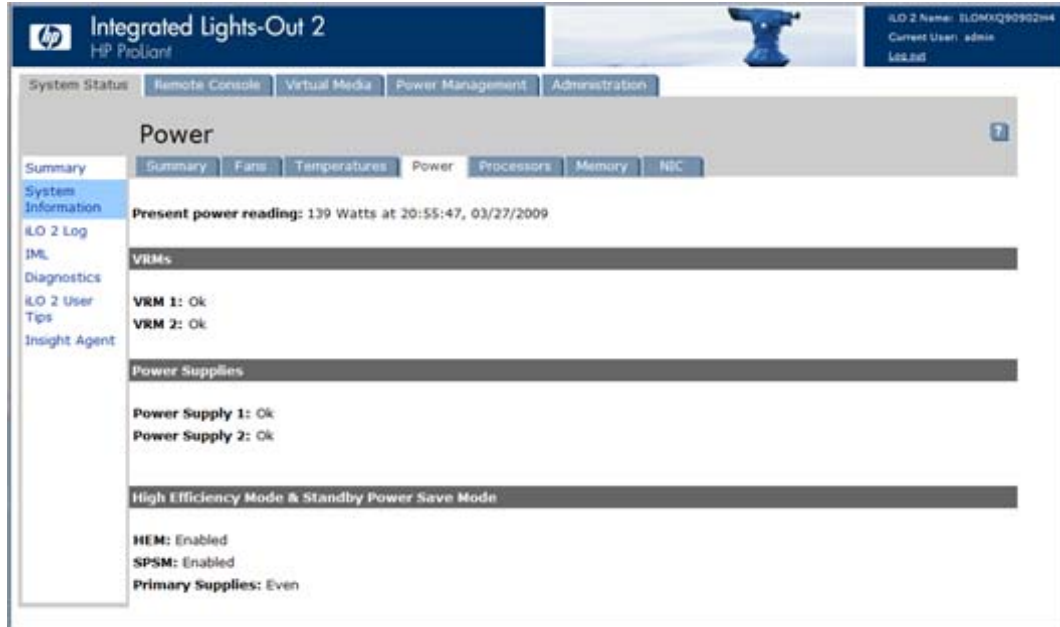
iLO2 consente di implementare un utilizzo di alimentazione migliorato utilizzando la modalità ad alta efficienza di alimentazione (HEM, High Efficiency Mode). La modalità HEM consente di migliorare l'efficienza di alimentazione ponendo gli alimentatori secondari in modalità di attesa. Quando gli alimentatori secondari sono in modalità di attesa, gli alimentatori principali forniscono tutta l'alimentazione CC al sistema. Gli alimentatori sono più efficienti (maggior quantità di watt di output CC per ogni watt di input CA) a maggiori livelli di output di alimentazione migliorando l'efficienza globale di alimentazione.

Quando il sistema assorbe più del 70% della capacità della potenza massima di output degli alimentatori principali, gli alimentatori secondari riprendono il normale funzionamento uscendo dalla modalità di attesa. Quando la potenza scende sotto il 60% della capacità degli alimentatori principali, gli alimentatori secondari ritornano in modalità di attesa. La modalità HEM consente di ottenere un consumo energetico pari al massimo output energetico degli alimentatori principali e secondari mantenendo al tempo stesso una migliore efficienza a livelli inferiori di utilizzo dell'alimentazione.

La modalità non influenza l'alimentazione ridondante. In caso di guasto dell'alimentatore principale, l'alimentatore secondario inizia immediatamente a fornire l'alimentazione CC al sistema prevenendo qualsiasi periodo di inattività.

La modalità HEM può essere configurata solo tramite RBSU. Queste impostazioni non possono essere modificate mediante iLO. Le impostazioni per la modalità HEM sono Enabled (Abilitato) o Disabled (Disabilitato), denominata anche Balanced Mode (Modalità bilanciata) e alimentatori Odd (Dispari) o Even (Pari) come principali. Queste impostazioni sono disponibili nella sezione High Efficiency Mode & Standby Power Save Mode (Modalità alta efficienza e modalità di risparmio energia in standby) della scheda System Information>Power (Informazioni di sistema>Alimentazione). Questa sezione presenta le seguenti informazioni:

- Se la modalità HEM è abilitata o disabilitata
- Quali alimentatori sono quelli principali (se la modalità HEM è abilitata)

- Quali alimentatori non supportano la modalità HEM

Arresto normale

La possibilità del microprocessore iLO 2 di eseguire un arresto normale dipende dalla cooperazione del sistema operativo. Affinché venga eseguito un arresto normale, è necessario che il driver di sicurezza sia installato. Grazie alla comunicazione tra iLO 2 e il driver, viene eseguito il metodo del sistema operativo più appropriato per arrestare il sistema in modo sicuro e garantire l'integrità dei dati.

Se il driver di sicurezza non è installato, il processore iLO 2 tenta di utilizzare il sistema operativo per eseguire un arresto normale tramite il pulsante di alimentazione. iLO 2 emula infatti un pulsante fisico di alimentazione per richiedere al sistema operativo di eseguire un arresto normale. Il comportamento del sistema operativo dipende dalla configurazione e dalle impostazioni relative alla pressione del pulsante di alimentazione.

La configurazione EAAS di HOST ROM RBSU consente di disabilitare questa funzionalità di arresto automatico. La disabilitazione dell'arresto automatico non è però consentita nelle condizioni più estreme, dove è presente il rischio di danneggiamento fisico del sistema.

A partire da Windows Server® 2003, i criteri di gruppo dei computer consentono il normale arresto del sistema con una pressione momentanea solo se un amministratore è collegato al sistema operativo. Per modificare questa impostazione e consentire sempre il normale arresto del sistema, effettuare le seguenti operazioni:

1. Al prompt dei comandi, eseguire il comando `gpedit.misc`.
2. Selezionare Configurazione computer>Impostazioni di Windows>Impostazioni protezione>Criteri locali>Opzioni di protezione>Arresto del sistema: in questo modo è possibile eseguire l'arresto del sistema senza dover accedere a **Attivato**.

Gestione avanzata di ProLiant BL p-Class

iLO 2 Advanced è un componente standard dei server blade ProLiant BL p-Class che garantisce la sicurezza del server e la gestibilità dei server blade a distanza. Alle relative funzioni è possibile accedere da un client di rete mediante un browser Web supportato. Oltre a fornire funzioni aggiuntive, iLO 2

Advanced consente di gestire la tastiera, il mouse e il video (testo e grafica) per un server blade, indipendentemente dallo stato del sistema operativo host o del server host di tipo blade.

In iLO 2 sono disponibili un microprocessore intelligente, memoria di sicurezza e un'interfaccia di rete dedicata. In base a questa configurazione, il sistema iLO 2 è indipendente dal server blade host e dal relativo sistema operativo. Il sistema iLO 2 consente inoltre di accedere in modalità remota a qualsiasi client di rete autorizzato e di inviare avvisi e fornisce altre funzionalità di gestione del server blade.

Utilizzando un browser Web supportato è possibile:

- Accedere in modalità remota alla console del server host e a tutte le schermate visualizzate in modalità grafica e in modalità testo con controlli completi di mouse e tastiera.
- Eseguire l'accensione, lo spegnimento o il riavvio del server blade host in modalità remota.
- Avviare in remoto un server host da un'immagine floppy virtuale per eseguire un aggiornamento della ROM o per installare un sistema operativo.
- Inviare avvisi da iLO 2 Advanced indipendentemente dallo stato del server blade host.
- Accedere alle funzionalità avanzate di risoluzione dei problemi disponibili in iLO 2 Advanced.
- Avviare un browser Web, usare gli allarmi SNMP ed eseguire la diagnostica del server blade mediante HP Systems Insight Manager.
- Configurare le impostazioni degli alloggiamenti con IP statico per i NIC di gestione iLO 2 dedicati su ogni server blade di un contenitore per eseguire l'implementazione in modo più rapido.

Il server blade deve essere collegato correttamente per la connettività iLO 2. Collegare il server blade utilizzando uno dei metodi indicati di seguito:

- Tramite una rete esistente (nel rack). Questo metodo richiede di installare il server blade nel relativo contenitore e di assegnarli un indirizzo IP (manualmente oppure utilizzando il protocollo DHCP).
- Tramite la porta I/O del server blade
  - Nel rack. Questo metodo richiede di collegare il cavo I/O locale alla porta I/O e a un PC client. Utilizzando l'indirizzo IP statico riportato sull'etichetta del cavo I/O e le informazioni di accesso disponibili nella parte anteriore del server blade, è possibile accedere a quest'ultimo mediante la console remota di iLO 2 Advanced.
  - Fuori dal rack, con la stazione di diagnostica: questo metodo richiede di alimentare il server blade con la stazione di diagnostica opzionale e di collegarsi a un computer esterno usando l'indirizzo IP statico e il cavo I/O locale. Per le istruzioni sul cablaggio, consultare la documentazione fornita con la stazione di diagnostica o il CD di documentazione.
  - Tramite i connettori del pannello posteriore del server blade (fuori dal rack, con la stazione di diagnostica). Questo metodo consente di configurare un server blade fuori dal rack alimentando il blade con la stazione di diagnostica e collegandosi a una rete esistente tramite un hub. L'indirizzo IP viene assegnato da un server DHCP su una rete.

La scheda BL p-Class consente di controllare le impostazioni specifiche del rack del server blade ProLiant BL p-Class. iLO 2 comprende inoltre funzioni di stato basate sul Web per il rack del server ProLiant BL p-Class.

Schermata Rack View

La schermata Rack View (Visualizzazione rack) fornisce una panoramica di tutti i contenitori, nonché dei server blade, dei componenti di rete e degli alimentatori in essi contenuti. Un componente presente nel rack viene visualizzato come componente selezionabile nella pagina Rack View (Visualizzazione rack). Non è possibile selezionare gli alloggiamenti vuoti. Le informazioni specifiche sui vari componenti,

quali nome del blade, indirizzo IP e tipo di prodotto, vengono visualizzate quando si posiziona il cursore del mouse su ciascun componente. Se si fa clic sul componente, informazioni aggiuntive e opzioni di configurazione vengono visualizzate nella schermata adiacente.

Nella schermata Rack View (Visualizzazione rack) sono disponibili i seguenti campi:

- Nome del rack
- Logged-in iLO Location (Posizione della connessione a iLO)

  In questo campo viene indicato il server a cui si è connessi. Per questo blade è possibile configurare solo le impostazioni del server.
- Selected Bay Location (Posizione dell'alloggiamento selezionato)

  In questo campo viene indicato l'alloggiamento selezionato. È possibile visualizzare le informazioni relative a numerosi tipi di componenti differenti, quali blade, alimentatori, componenti di rete e contenitori.
- Enclosure Details (Dettagli dei contenitori)

  Informazioni relative a un contenitore specifico possono essere visualizzate selezionando **Dettagli** accanto alle intestazioni dei contenitori numerati.

Il pulsante Refresh (Aggiorna) consente di ottenere informazioni aggiornate sul rack. Fare clic su **Refresh** (Aggiorna) per aggiornare l'intera rappresentazione grafica del rack. Questo processo richiede alcuni minuti.

Qualora non sia possibile ottenere le informazioni corrette sul rack, invece dei componenti viene visualizzato un messaggio di errore. È possibile usare il pulsante Refresh (Aggiorna) per tentare nuovamente di ottenere i dati corretti. Per una visualizzazione corretta, la funzionalità Rack View (Visualizzazione rack) richiede la versione 2.10, o una versione successiva, del firmare del server blade e del modulo di gestione dell'alimentazione.

Configurazione e informazioni del blade

L'opzione di configurazione del blade fornisce informazioni sull'identità, la posizione e l'indirizzo di rete del blade selezionato nella pagina Rack View (Visualizzazione rack). Per visualizzare queste impostazioni, selezionare un componente del blade, quindi fare clic su **Configure** (Configura) nella pagina relativa alla visualizzazione del rack (Schermata Rack View a pagina 132). È possibile modificare alcune delle impostazioni relative al server blade a cui è connesso l'utente. Per salvare le modifiche, fare clic su **Applica** (Applica).

Sono disponibili i seguenti campi:

- Identification Information (Informazioni di identificazione)
  - Bay Name (Nome dell'alloggiamento)
  - Bay Number (Numero di alloggiamento)
- Power On Control (Controllo accensione)
  - Power Source (Fonte di alimentazione)
  - Enable Automatic Power On (Abilita accensione automatica)
  - Enable Rack Alert Logging (IML) (Abilita registrazione allarmi del rack (IML))

Informazioni dei contenitori

Le informazioni dei contenitori si riferiscono al contenitore selezionato. Informazioni relative a un contenitore specifico possono essere visualizzate selezionando **Dettagli** accanto alle intestazioni dei contenitori numerati. È disponibile una quantità limitata di informazioni sul rack, tra cui il nome e il numero di serie.

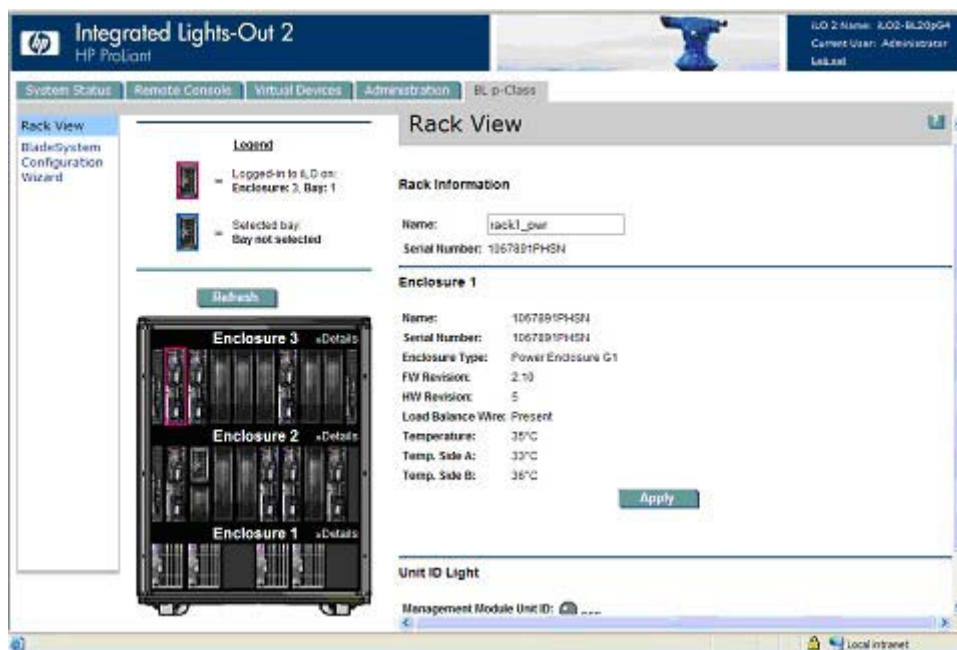
Sono inoltre disponibili alcune informazioni sui contenitori che non includono il server blade a cui si è connessi. Queste informazioni comprendono il nome, il numero di serie e il tipo di contenitore.

Per il contenitore in cui è presente l'alloggiamento a cui si è connessi è invece disponibile un'ampia gamma di informazioni. Queste informazioni comprendono:

- Nome
- Numero di serie
- Tipo di contenitore
- Revisione del firmware
- Revisione dell'hardware
- Temperatura del contenitore
- ID dell'unità del modulo di gestione

Alcuni campi possono essere modificati e aggiornati facendo clic sul pulsante **Apply** (Applica).

Informazioni del contenitore di alimentazione

La pagina relativa alle informazioni del contenitore di alimentazione fornisce informazioni di diagnostica riguardo al modulo di gestione dell'alimentazione e ai componenti di alimentazione presenti nel contenitore di alimentazione. Queste informazioni forniscono una panoramica sullo stato e sulla condizione del contenitore e dei componenti di alimentazione.

Sono disponibili le seguenti informazioni:

- Nome del rack
- Numero di serie del rack
- Nome del contenitore
- Numero di serie contenitore
- Tipo di contenitore
- Revisione del firmware
- Revisione dell'hardware
- Filo per il bilanciamento del carico
- Temperatura del contenitore
- Temperatura dei lati A e B del contenitore
- ID dell'unità del modulo di gestione

Alcuni campi possono essere modificati e aggiornati facendo clic sul pulsante **Apply** (Applica).

Informazioni dei componenti di rete

Le informazioni dei componenti di rete indicano lo stato del pannello delle patch o dell'interruttore di interconnessione selezionato. Le informazioni visualizzate comprendono Fuse A (Fusibile A), Fuse B (Fusibile B) e Network Component Type (Tipo componente di rete).

Controllo iLO 2 dei LED del server ProLiant BL p-Class

iLO 2 è in grado di monitorare i server BL p-Class tramite il controller del POST e il LED di sicurezza del server.

Controller del POST del server

Poiché i server ProLiant BL p-Class non dispongono di tastiera, mouse e video, il riscontro fornito all'avvio è limitato. iLO 2 supplisce a questa mancanza mediante il LED di sicurezza del server che lampeggia durante il POST. Se l'avvio non ha esito positivo, il LED si accende in modo fisso con colore ambra. Se invece l'avvio termina correttamente, il LED si accende in modo fisso nel colore verde.

Dopo un avvio riuscito, il controllo del LED di sicurezza del server viene restituito al server, che potrebbe spegnere il LED o accenderlo in un altro colore per rappresentare lo stato dell'hardware del server.

Avviso di alimentazione insufficiente

iLO 2 accende il LED di sicurezza del server in modo fisso nel colore rosso se non è in grado di accendere il server a causa dell'alimentazione insufficiente nell'infrastruttura del rack.

Inoltro d'allarmi per ProLiant BL p-Class

iLO 2 supporta i trap SNP dell'infrastruttura blade in base al pass-through. La segnalazione dello stato dell'infrastruttura blade di iLO 2 non richiede supporto dal sistema operativo. Gli allarmi (trap) vengono creati dai gestori del contenitore e dell'alimentatore e vengono trasmessi a iLO 2. Il firmware p-Class di iLO 2 inoltra gli allarmi di infrastruttura come trap SNMP a una console di gestione configurata correttamente. Questi allarmi consentono di monitorare gli allarmi p-Class da una console di gestione SNMP.

L'inoltro di allarmi p-Class viene disabilitata per impostazione predefinita e può essere abilitata dalla pagina Web SNMP/Insight Manage Settings.

I seguenti messaggi di allarme vengono identificati e inoltrati da iLO 2:

ID allarme	Descrizione
22005	Errore di temperatura del contenitore
22006	Degradazione della temperatura del contenitore
22007	Temperatura del contenitore OK
22008	Errore della ventola del contenitore
22009	Degradazione della ventola del contenitore
22010	Ventola del contenitore OK
22013	Errore dell'alimentazione del rack
22014	Degradazione dell'alimentazione del rack
22015	Alimentatore del rack OK
22023	Errore del server rack; alimentazione non sufficiente

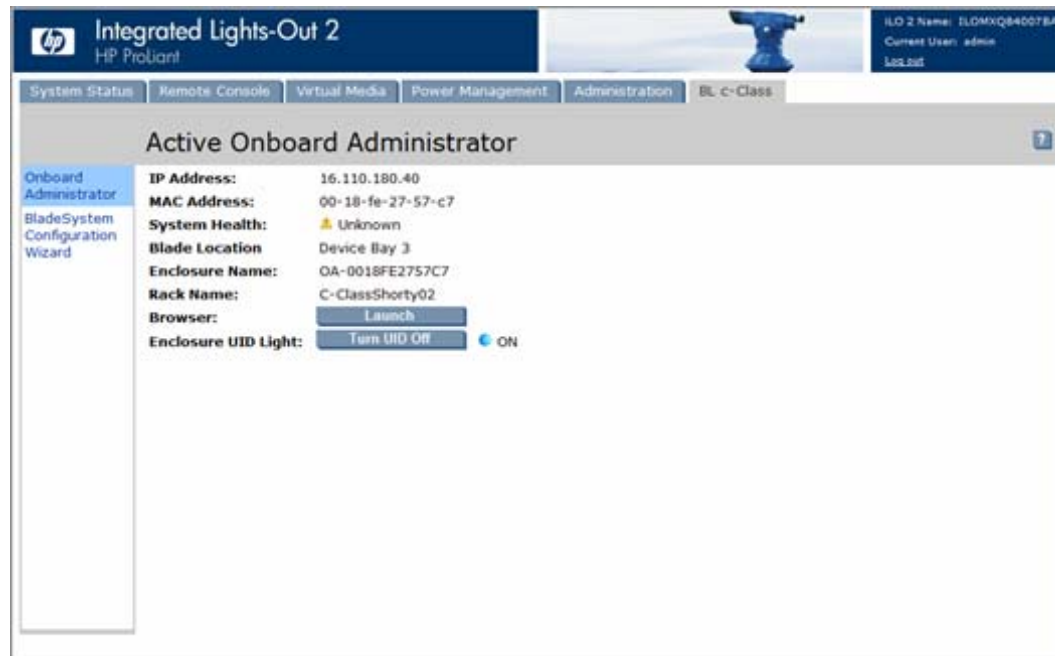
HP BladeSystem Onboard Administrator per ProLiant

HP BladeSystem Onboard Administrator è composto da processore, sottosistema e firmware per la gestione del contenitore e viene utilizzato per supportare HP BladeSystem e tutti i dispositivi gestiti all'interno del contenitore.

È possibile accedere a iLO 2 mediante l'opzione iLO di HP Onboard Administrator (Opzione iLO a pagina 142) direttamente o selezionando il collegamento Web Administration (Amministrazione tramite Web) (Amministrazione tramite Web a pagina 143). Per ulteriori informazioni su come accedere

direttamente a iLO 2, vedere la sezione "Primo accesso a iLO 2" (Primo accesso a iLO 2 a pagina 12).

Scheda BL c-Class di iLO 2

Dalla scheda BL c-Class dell'interfaccia Web di iLO 2 è possibile accedere a Onboard Administrator e alla configurazione guidata di BladeSystem. Per ulteriori informazioni sulla configurazione guidata di BladeSystem, consultare la *Guida utente di HP BladeSystem Onboard Administrator*.

L'opzione Onboard Administrator consente di visualizzare una breve panoramica dello stato del sistema del server, avviare un browser con la schermata Rack View (Visualizzazione rack) di HP Onboard Administrator o accendere e spegnere gli indicatori UID.

Indirizzamento IP degli alloggiamenti del contenitore

Al completamento della procedura guidata di configurazione First Time Setup Wizard viene chiesto di configurare l'indirizzamento IP degli alloggiamenti del contenitore. Per ulteriori informazioni sull'intero processo di questa configurazione guidata, consultare la *Guida utente di HP BladeSystem Onboard Administrator*.

Gli indirizzi IP per le porte iLO 2 del server blade e per le porte di gestione dei moduli di interconnessione possono essere ottenuti in tre modi: indirizzi DHCP, indirizzi IP statici o EBIPA (Enclosure Bay IP Addressing, Indirizzamento IP degli alloggiamenti del contenitore). Se la rete dispone di un servizio

DHCP esterno o se si desidera assegnare manualmente i singoli indirizzi IP statici a ciascun server blade e modulo di interconnessione, fare clic su **Skip** (Ignora) per non eseguire il presente passaggio.

- Indirizzi DHCP – Per impostazione predefinita per il server blade viene impostato l'indirizzamento DHCP mediante il connettore di rete del modulo Onboard Administrator attivo. Anche per i moduli di interconnessione che dispongono di una connessione di rete di gestione interna a Onboard Administrator è possibile utilizzare l'indirizzamento DHCP per impostazione predefinita.

  Nell'interfaccia grafica di Onboard Administrator sono riportati gli indirizzi IP per la porta iLO 2 del server blade e per la porta di gestione dei moduli di interconnessione.

- IP statico
  - Manuale – Se si preferisce assegnare indirizzi IP statici, è possibile impostare separatamente tutte le porte iLO 2 dei server blade e le porte di gestione dei moduli di interconnessione su indirizzi statici univoci oppure utilizzare EBIPA per assegnare un intervallo di indirizzi IP statici ai singoli alloggiamenti dei server blade e dei moduli di gestione.
  - EBIPA – Quando un server blade o un modulo di interconnessione viene inserito in un alloggiamento per cui EBIPA è stato abilitato, Onboard Administrator assegna alla relativa porta di gestione un indirizzo IP statico specifico, se il dispositivo è configurato per DHCP.

Utilizzando la configurazione guidata EBIPA di Onboard Administrator, l'amministratore imposta un intervallo indipendente per gli alloggiamenti dei server blade e per gli alloggiamenti dei moduli di interconnessione. Al primo alloggiamento viene assegnato il primo indirizzo nell'intervallo, quindi vengono assegnati in maniera sequenziale gli indirizzi degli altri alloggiamenti.

Ad esempio, se l'intervallo EBIPA dell'alloggiamento del server viene impostato tra 16.100.226.21 e 16.100.226.36, all'iLO 2 nell'alloggiamento del dispositivo n. 1 sarà assegnato l'indirizzo 16.100.226.21, mentre all'iLO 2 nell'alloggiamento del dispositivo n. 12 sarà assegnato l'indirizzo 16.100.226.36. Se l'intervallo EBIPA dell'alloggiamento di interconnessione viene impostato tra 16.200.139.51 e 16.209.139.58, alla porta di gestione dei moduli di interconnessione nell'alloggiamento di interconnessione n. 1 sarà assegnato l'indirizzo 16.200.139.51, mentre alla porta di gestione dei moduli di interconnessione nell'alloggiamento di interconnessione n. 7 sarà assegnato l'indirizzo 16.200.139.57.

Per abilitare le impostazioni EBIPA per gli alloggiamenti del server in questo contenitore, selezionare **Enable Enclosure Bay IP Addressing for Server Bay iLO 2 Processors** (Abilita indirizzamento IP per alloggiamenti contenitore per processori iLO 2 di alloggiamenti server), quindi immettere le informazioni riportate di seguito.

Campo	Valore possibile	Descrizione
Beginning Address (Indirizzo di inizio)	###.###.###.###, dove ### è un valore compreso tra 0 e 255.	L'indirizzo IP di inizio per gli alloggiamenti dei dispositivi o dei moduli di interconnessione. Fare clic sulla freccia vicino al campo Beginning Address (Indirizzo di inizio) e fare clic su **Update List** (Aggiorna elenco) per aggiornare l'elenco dei dispositivi e l'elenco dei moduli di interconnessione.
Maschera di sottorete	###.###.###.###, dove ### è un valore compreso tra 0 e 255.	Maschera di sottorete per gli alloggiamenti dei dispositivi o dei moduli di interconnessione.
Gateway	###.###.###.###, dove ### è un valore compreso tra 0 e 255.	L'indirizzo del gateway per gli alloggiamenti dei dispositivi o dei moduli di interconnessione.
Dominio	Una stringa di caratteri, inclusi tutti i caratteri alfanumerici e il trattino (-).	Il nome del dominio per gli alloggiamenti dei dispositivi o dei moduli di interconnessione.

Campo	Valore possibile	Descrizione
DNS Server 1 (Server DNS 2)	###.###.###.###, dove ### è un valore compreso tra 0 e 255.	L'indirizzo IP del server DNS primario.
DNS Server 2 (Server DNS 2)	###.###.###.###, dove ### è un valore compreso tra 0 e 255.	L'indirizzo IP del server DNS secondario.
DNS Server 3 (Server DNS 2)	###.###.###.###, dove ### è un valore compreso tra 0 e 255.	L'indirizzo IP del server DNS terziario.
NTP Server 1 (Server NTP 2)	###.###.###.###, dove ### è un valore compreso tra 0 e 255.	L'indirizzo IP del server primario utilizzato per la sincronizzazione di data e ora mediante il protocollo NTP.
NTP Server 2 (Server NTP 2)	###.###.###.###, dove ### è un valore compreso tra 0 e 255.	L'indirizzo IP del server secondario utilizzato per la sincronizzazione di data e ora mediante il protocollo NTP.

Limitazione dell'alimentazione dinamica per server blade

La limitazione dell'alimentazione dinamica è una funzionalità di iLO 2 disponibile per server blade c-Class a cui è possibile accedere tramite HP Onboard Administrator. Per ulteriori informazioni sulle opzioni di impostazione dell'alimentazione disponibili per server blade c-Class, consultare la *Guida utente di HP BladeSystem Onboard Administrator*.

La limitazione dell'alimentazione dinamica è disponibile solo se la piattaforma hardware del sistema, BIOS (ROM), e il firmware del microcontroller di tensione supportano questa funzione. Se nel sistema è possibile attivare la limitazione dell'alimentazione dinamica, iLO 2 viene automaticamente impostato sulla modalità di limitazione dell'alimentazione dinamica.

In Onboard Administrator sono disponibili due opzioni di limitazione dell'alimentazione dinamica:

- Dynamic Power (Alimentazione dinamica)

  Scegliendo questa opzione, viene attivata la modalità Standby per gli alimentatori non utilizzati, aumentando l'efficienza energetica del contenitore e riducendo il consumo nei periodi di minore richiesta energetica. In caso di aumento della richiesta energetica, la modalità Standby verrebbe automaticamente disattivata e verrebbe ripristinato il pieno funzionamento degli alimentatori. Se l'alimentazione dinamica è:

  - Enabled (Abilitato) - È possibile che alcuni degli alimentatori vengano automaticamente posti in standby per aumentare l'efficienza complessiva del sottosistema di alimentazione del contenitore (impostazione predefinita).
  - Disabled (Disabilitato) - Il carico viene suddiviso tra tutti gli alimentatori. L'efficienza del sottosistema di alimentazione varia in base all'entità del carico.

- Enclosure Dynamic Power Cap (Limite alimentazione dinamica contenitore)

  Impostazione opzionale che consente di stabilire un limite per un gruppo di server all'interno di un contenitore. Impostare il limite entro i valori visualizzati al di sopra del campo Enclosure Dynamic Power Cap (Limite alimentazione dinamica contenitore). Questi valori sono basati sulla configurazione corrente del contenitore.

  Quando i server sono in funzione, la richiesta energetica varia per ciascuno di essi. Per ognuno viene quindi impostato un limite, in modo tale che al server sia fornita alimentazione sufficiente per soddisfare i fabbisogni del carico di lavoro, rispettando al contempo il valore Enclosure Dynamic Power Cap (Limite alimentazione dinamica contenitore).

È possibile utilizzare le impostazioni Static Power Limit (Limite alimentazione statico) o Enclosure Dynamic Power Cap (Limite alimentazione dinamica contenitore) nei seguenti casi:

◦ Se l'alimentazione di rete è limitata al contenitore, è possibile impostare un limite fisso per ogni contenitore. Si supponga, ad esempio, che in un ambiente hosting l'alimentazione del contenitore venga limitata a 5000 W. In questo caso, Onboard Administrator limiterà l'allocazione complessiva di energia a 5.000 W, limitazione che potrebbe determinare una mancanza di energia per alcuni dei server blade.

◦ Se la struttura limita la capacità di raffreddamento del contenitore, dividere per 3,41 il limite di Btu/hr disponibile per il contenitore per determinare il limite in watt per tale contenitore. Immettere il limite in watt per ridurre il carico di riscaldamento dei contenitori. Ad esempio: la struttura limita ogni contenitore a 27.280 Btu/hr, dividendo 27.280 per 3,41 si ottiene 8000 W. Immettere questo valore per limitare il contenitore in oggetto a 27.280 Btu/hr. In questo modo, tuttavia, alcuni dei server blade potrebbero non ricevere l'alimentazione necessaria.

◦ Se si desidera limitare la temperatura in uscita o il carico elettrico del contenitore, è preferibile utilizzare l'impostazione Enclosure Dynamic Power Cap. Rispetto all'impostazione Static Power Limit, consente infatti di alimentare un maggior numero di server blade. Si consiglia invece di utilizzare Static Power Limit nei casi seguenti:

  — Non si desidera una regolazione dinamica dei limiti per i server blade.

  — Si preferisce non attivare un server blade se non è possibile alimentarlo correttamente (anche se in genere consuma meno).

  — Più di 1/4 dei server blade nel contenitore non soddisfano i requisiti relativi a hardware o firmware per l'opzione Enclosure Dynamic Power Cap.

  — Non si dispone di alimentatori CA ridondanti.

  — Non impostare limiti per un contenitore vuoto. Questa operazione disabilita entrambe le opzioni Static Power Limit ed Enclosure Dynamic Power Cap.

Per ulteriori informazioni sull'opzione Static Power Limit, consultare la *Guida utente di HP BladeSystem Onboard Administrator*.

Ventola virtuale di iLO 2

Nei server blade c-class, HP Onboard Administrator controlla le ventole del contenitore. Il firmware di iLO 2 non è in grado di rilevare queste ventole. Il firmware di iLO 2 esegue invece il monitoraggio di un sensore della temperatura ambientale situato sul server blade. Le informazioni sulla temperatura vengono visualizzate nell'interfaccia di iLO 2 e recuperate periodicamente da Onboard Administrator. HP Onboard Administrator utilizza le informazioni del sensore raccolte da tutti i processori di gestione iLO 2 presenti nel contenitore per determinare la velocità delle ventole del contenitore.

Opzione iLO

L'opzione iLO di HP Onboard Administrator consente di accedere alla funzionalità di amministrazione tramite Web di iLO 2 (Amministrazione tramite Web a pagina 143), alla console remota integrata a schermo intero (Console remota integrata a schermo intero a pagina 92), alla console remota integrata (Console remota integrata a pagina 92), alla console remota e alla console seriale remota (Console seriale remota a pagina 108). La selezione di un collegamento in questa sezione apre la relativa sessione iLO in una nuova finestra utilizzando SSO, che non richiede l'immissione di un nome utente o una password iLO.

Se in base alle impostazioni del browser non è consentito aprire nuove finestre, i collegamenti non funzioneranno correttamente. Per informazioni su come disattivare il blocco delle finestre a comparsa, consultare la Guida in linea.

Amministrazione tramite Web

Il collegamento Web Administration (Amministrazione tramite Web) all'interno di HP Onboard Administrator consente di accedere all'interfaccia grafica di iLO 2, visualizzando la pagina System Status (Stato sistema) contenente una panoramica dello stato del server.

Funzioni dei server BL p-Class e BL c-Class

Alcune delle funzioni dei server HP ProLiant BL p-Class e c-Class sono uguali. Nella tabella riportata di seguito sono elencate le principali differenze tra i due prodotti.

Funzione	BL c-Class	BL p-Class
Comunicazione tra contenitori	Ethernet	i2c

Funzione	BL c-Class	BL p-Class
Indirizzamento IP basato sul contenitore	DHCP	SBIPC
Autenticazione tra contenitore e iLO 2	Mutua	Non supportata
Ventola del server	Virtuale	Fisica
Configurazione e informazioni del server blade	Non limitate	Limitate
Accensione forzata	Non supportata	Supportata
Chiave hardware frontale	SUV (no iLO 2)	SUVi
Gestione del rack	Supporto completo mediante HP Onboard Administrator	Supporto limitato mediante iLO 2

5 Servizi di directory

In questa sezione

Panoramica dell'integrazione di directory

È possibile configurare iLO 2 in modo che utilizzi una directory per autenticare e autorizzare gli utenti. Prima di configurare iLO 2 per le directory, è necessario stabilire se si desidera utilizzare l'opzione relativa allo schema esteso HP.

I vantaggi derivanti dall'utilizzo dell'opzione relativa allo schema esteso HP sono i seguenti:

- Maggiore flessibilità nel controllo dell'accesso. Ad esempio, l'accesso può essere limitato a un determinato periodo del giorno o a un determinato intervallo di indirizzi HP.
- Gestione dei gruppi nella directory, non in ogni singolo iLO 2.
- RILOE e RILOE II funzionano soltanto con lo schema esteso HP. In futuro l'opzione senza schema verrà estesa a RILOE II.

iLO 2, RILOE e RILOE II funzioneranno soltanto con eDirectory e lo schema esteso HP.

Per un elenco completo dei vantaggi, vedere la sezione "Vantaggi dell'integrazione di directory " (Vantaggi dell'integrazione di directory a pagina 145). Nella sezione "Gestione remota abilitata alla directory" (Gestione remota abilitata alla directory a pagina 179) viene illustrato il modo in cui la sicurezza, i ruoli e i gruppi vengono abilitati e imposti mediante l'utilizzo di directory. Per ulteriori informazioni sull'integrazione di directory, è inoltre possibile consultare la documentazione disponibile sul sito Web HP (http://www.hp.com/servers/lights-out).

Vantaggi dell'integrazione di directory

- Scalabilità – È possibile utilizzare la directory in modo da supportare migliaia di utenti su migliaia di iLO 2.
- Protezione – Vengono applicati criteri di password estremamente rigorosi già utilizzati nelle directory. Si applicano ad esempio i criteri di complessità delle password, di frequenza di rotazione e di scadenza.
- Anonimato (mancanza di) – In alcuni ambienti, gli utenti condividono gli account Lights-Out e ciò impedisce di conoscere con precisione chi ha eseguito le varie operazioni, anziché sapere qual è l'account o il ruolo utilizzato.

- Gestione basata sul ruolo – È possibile creare vari ruoli, ad esempio utenti d'ufficio, controllo remoto dell'host, controllo completo, e associarvi utenti o gruppi di utenti. Le modifiche apportate a un ruolo si applicano quindi a tutti gli utenti e ai dispositivi Lights-Out che vi sono associati.
- Punto unificato di amministrazione – Per gestire gli utenti Lights-Out è possibile utilizzare strumenti di amministrazione originari come MMC e ConsoleOne.
- Immediatezza – Una singola modifica apportata alla directory viene estesa immediatamente a tutti i processori Lights-Out associati. In tal modo, si elimina la necessità di gestire il processo tramite script.
- Eliminazione di altri nomi utenti e password – È possibile utilizzare gli account utente e le password esistenti nella directory senza dover registrare o memorizzare nuove credenziali per Lights-Out.
- Flessibilità – È possibile creare un singolo ruolo per un singolo utente su un singolo iLO 2 oppure creare un singolo ruolo per più utenti su più iLO 2 oppure utilizzare combinazioni di ruoli basate sulle esigenze aziendali.
- Compatibilità – L'integrazione delle directory Lights-Out si applica ai prodotti iLO 2, RILOE e RILOE II. L'integrazione supporta Active Directory ed eDirectory.
- Standard – Le directory Lights-Out supportano versioni successive allo standard LDAP 2.0 per l'accesso sicuro.

Vantaggi e svantaggi dei metodi di integrazione di directory senza schema e con schema HP

Consentendo la gestione dei diritti e degli accessi da una posizione centralizzata, le directory contribuiscono a migliorare il livello di protezione. Le directory assicurano inoltre una considerevole flessibilità di configurazione. Quando si utilizza iLO 2, alcune procedure di configurazione delle directory risultano più efficaci di altre. Prima di eseguire la configurazione di iLO 2 per le directory, è necessario decidere se si preferisce utilizzare il metodo di integrazione di directory con schema HP o senza schema. Rispondendo alle domande riportate di seguito, è possibile comprendere meglio le proprie esigenze in termini di integrazione di directory.

1. È possibile applicare estensioni di schema alla propria directory?
   - No – Si sta utilizzando Microsoft Active Directory?
   - No – L'integrazione di directory può non essere adatta al proprio ambiente. Considerare la possibilità di installare un server di directory di valutazione per esaminare i possibili vantaggi offerti dall'integrazione di directory.

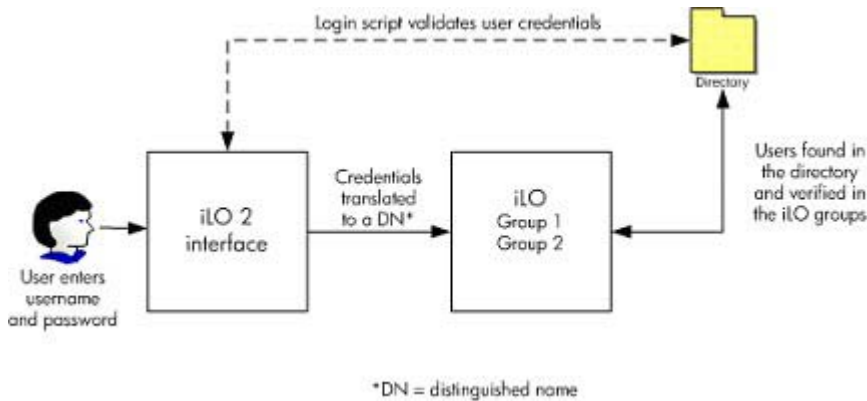
     — Sì – Utilizzare il metodo di integrazione di directory senza schema basato su gruppi.
   - Sì – Procedere con la seconda domanda.
2. Che grado di scalabilità offre la propria configurazione?
   - No – Installare un'istanza del processo di integrazione di directory senza schema per valutare se questo metodo di integrazione risponde ai requisiti procedurali e ai criteri di sicurezza personali. Se necessario, è possibile utilizzare il metodo di integrazione di directory con schema HP in un secondo momento.
   - Sì – Utilizzare il metodo di integrazione di directory con schema HP.

     Le domande riportate di seguito possono contribuire a determinare se la configurazione corrente è scalabile:
   - Si prevede di dover modificare i diritti o i privilegi di un gruppo di utenti della directory?

◦ Si esegue regolarmente lo script delle modifiche apportate a iLO 2?

◦ Si utilizzano più di cinque gruppi per controllare i privilegi di iLO 2?

Integrazione delle directory senza schema

Se si utilizza il metodo di integrazione directory senza schema, gli utenti e le appartenenze ai gruppi risiedono nella directory, mentre i privilegi dei gruppi si trovano in iLO 2. Utilizzando le credenziali di accesso, iLO 2 accede all'oggetto utente nella directory e rileva le appartenenze degli utenti ai gruppi, che vengono quindi confrontate con quelle memorizzate in iLO 2. In caso di corrispondenza, l'autorizzazione viene concessa. Ad esempio:

Vantaggi del metodo di integrazione di directory senza schema:

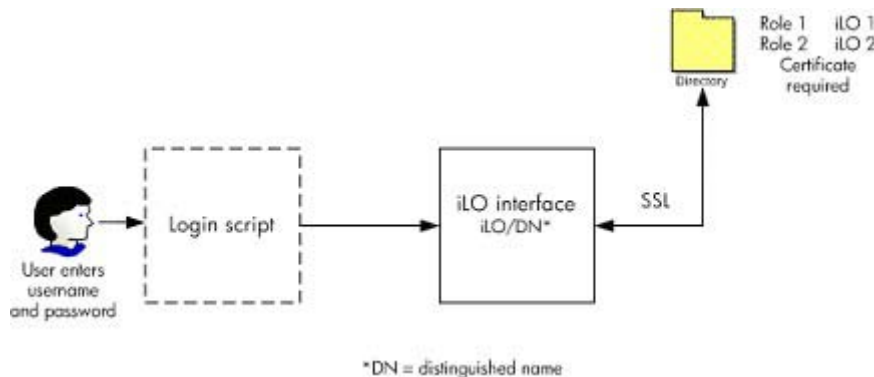
- Non è necessario estendere lo schema della directory.
- Viene supportato l'accesso mediante NetBIOS e formati di posta elettronica, se i controlli ActiveX sono abilitati nel browser.
- Non è richiesta la configurazione, o è richiesta una configurazione minima, da parte degli utenti nella directory. Se non è richiesta alcuna procedura di configurazione, per accedere a iLO la directory utilizza gli utenti e le appartenenze ai gruppi esistenti. Se ad esempio è stato definito un amministratore di dominio denominato User1, è possibile copiare in iLO 2 il nome distinto del gruppo di protezione dell'amministratore di dominio e concedergli privilegi completi. In questo modo, User1 può accedere a iLO 2.

Svantaggi del metodo di integrazione di directory senza schema:

- Supporta solo Microsoft® Active Directory.
- I privilegi dei gruppi vengono amministrati a livello di singolo iLO 2. Questo svantaggio, tuttavia, viene parzialmente annullato dal fatto che i privilegi dei gruppi vengono modificati raramente e che l'attività di modifica delle appartenenze ai gruppi viene amministrata a livello di directory e non di singolo iLO 2. HP mette a disposizione strumenti che consentono di apportare modifiche su più iLO 2 contemporaneamente.

Integrazione delle directory tramite schema HP

L'integrazione di directory con schema HP è composta da una classe denominata hpqRole (sottoclasse di Group) e di una classe denominata hpqTarget (sottoclasse di User), oltre ad altre classi del programma di aiuto. Un'istanza della classe hpqRole è semplicemente un ruolo, mentre un'istanza della classe hpqTarget è equivalente a un iLO 2.

A ogni ruolo sono associati uno o più iLO 2 e uno o più utenti ed è assegnato un elenco di privilegi che gli utenti possono utilizzare su iLO 2 nel ruolo. Tutti gli accessi a iLO 2 vengono gestiti aggiungendo e rimuovendo dal ruolo utenti e unità iLO 2, nonché gestendo i privilegi nel ruolo. Ad esempio:

Vantaggi del metodo di integrazione di directory con schema HP:

- Maggiore flessibilità nel controllo degli accessi. Ad esempio, è possibile limitare l'accesso a un determinato periodo del giorno o a un determinato intervallo di indirizzi HP.
- I gruppi e i permessi vengono gestiti a livello di directory, non di singolo iLO 2. HP fornisce inoltre gli snap-in necessari per la gestione di destinatari e gruppi HP sia per Utenti e computer di Active Directory che per eDirectory ConsoleOne.
- È consentita l'integrazione con eDirectory.

Svantaggi del metodo di integrazione di directory con schema HP:

- È necessaria un'estensione dello schema di directory. Questo svantaggio, tuttavia, viene parzialmente annullato dal fatto che HP mette a disposizione il file .ldf e una procedura guidata per l'estensione dello schema e che versioni successive di Active Directory consentiranno di annullare le modifiche apportate allo schema.

  Per informazioni sulla procedura di estensione dello schema e sulla configurazione delle impostazioni di directory, consultare il documento *Integrating HP ProLiant Lights-Out processors with Microsoft® Active Directory* (Integrazione dei processori HP ProLiant Lights-Out con Microsoft® Active Directory) (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00190541/c00190541.pdf).
- Requisiti di certificazione

  Per comunicare con la directory, iLO 2 deve utilizzare il protocollo LDAP su SSL. Questo tipo di comunicazione richiede tuttavia che sul server di directory sia installato un certificato. L'installazione del certificato per il dominio viene replicata su tutti i controller presenti nel dominio. Per informazioni sull'installazione del certificato, utilizzare il servizio Customer Advisory disponibile sul sito Web HP (http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp).
- Opzioni di failover

  Per abilitare il failover (ridondanza), utilizzare il nome di dominio come nome del server di directory durante la configurazione di iLO 2. La maggior parte dei server DNS è in grado di risolvere un nome di dominio in un server di directory funzionante (controller di dominio).
- Formato di accesso

  I formati dei nomi di accesso supportati comprendono NetBIOS, UPN e il nome distinto. Lo script di accesso per iLO 2 comunica con il sistema operativo client e tenta di tradurre il nome di accesso in un nome distinto per la directory. Affinché questa situazione si verifichi, è tuttavia necessario

che il nome della directory sia un nome DNS, non un indirizzo IP. È necessario anche che il client e iLO 2 possano accedere al server di directory utilizzando lo stesso nome. Devono trovarsi inoltre nello stesso dominio DNS.

- Destinatari multipli

  Non è necessario utilizzare destinatari multipli nella directory. L'integrazione di directory con schema HP richiede solo un oggetto hpqTarget, che può rappresentare più dispositivi LOM.

Configurazione dell'integrazione di directory senza schema

Prima di impostare l'opzione senza schema, il sistema deve soddisfare tutti i prerequisiti illustrati nella sezione "Preparazione di Active Directory" (Preparazione di Active Directory a pagina 149).

È possibile impostare iLO 2 per le directory in tre modi:

- Manualmente mediante l'utilizzo di un browser (Impostazione basata su browser senza schema a pagina 151).
- Utilizzando uno script (Configurazione senza schema tramite script a pagina 151).
- Utilizzando HPLOMIG (Impostazione senza schema basata su HPLOMIG a pagina 151).

Preparazione di Active Directory

L'opzione senza schema viene supportata nei seguenti sistemi operativi:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory

È necessario abilitare SSL nella directory. Per abilitare SSL, installare un certificato di dominio in Active Directory. iLO 2 comunica esclusivamente con la directory su un collegamento SSL protetto. Per ulteriori informazioni, consultare l'articolo della Knowledge Base Microsoft® 247078, *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers* disponibile sul sito Web Microsoft® all'indirizzo http://support.microsoft.com/.

Per convalidare la configurazione, è necessario avere il nome distinto di directory di almeno un utente e il nome distinto di un gruppo di protezione di cui l'utente è membro.

Introduzione a Servizi certificati

I Servizi certificati consentono di emettere certificati digitali firmati a host di rete. I certificati permettono di stabilire collegamenti SSL con l'host e di verificare l'autenticità di quest'ultimo.

L'installazione di Servizi certificati consente ad Active Directory di ricevere un certificato che permette ai processori Lights-Out di collegarsi al servizio di directory. Senza il certificato, iLO 2 non può collegarsi al server di directory.

Ogni server di directory a cui si desidera collegare iLO 2 deve avere un certificato. Se si installa Enterprise Certificate Service, Active Directory può richiedere e installare in modo automatico i certificati per tutti i controller Active Directory della rete.

Installazione di Servizi certificati

1. Selezionare **Start>Impostazioni>Panello di controllo**.
2. Fare doppio clic su **Installazione applicazioni**.

3. Fare clic su **Installazione componenti di Windows** per avviare l'Aggiunta guidata componenti di Windows.
4. Selezionare la casella di controllo **Servizi certificati**. Fare clic su **Avanti**.
5. Quando viene visualizzato l'avviso che non è possibile rinominare il server, fare clic su **OK**. L'opzione CA globale (enterprise) principale è selezionata perché non vi è alcun autorità di certificazione registrata nella directory attiva.
6. Immettere le informazioni appropriate per il sito e l'organizzazione. Accettare il periodo predefinito di due anni per il campo `Valido per`. Fare clic su **Avanti**.
7. Accettare il percorso predefinito del database di certificato e del log di database. Fare clic su **Avanti**.
8. Quando il sistema richiede il CD di Windows® 2000 Advanced Server, sfogliare fino alla cartella c:\I386.
9. Fare clic su **Fine** per chiudere la procedura guidata.

Verifica di Servizi certificati

I processori di gestione comunicano con Active Directory tramite SSL, pertanto è necessario creare un certificato o installare Servizi certificati. È necessario installare un'autorità di certificazione aziendale perché si emetteranno certificati a oggetti inclusi nel dominio dell'organizzazione.

Per verificare che Servizi certificati sia installato, selezionare **Start>Tutti i programmi>Strumenti di amministrazione>Autorità di certificazione**. Se Servizi certificati non è installato, viene visualizzato un messaggio di errore.

Configurazione della richiesta automatica certificati

Per specificare che un certificato deve essere rilasciato al server:

1. Selezionare **Start>Esegui** e digitare `mmc`.
2. Fare clic su **Aggiungi**.
3. Selezionare **Criteri di gruppo** e fare clic su **Aggiungi** per aggiungere lo snap-in a MMC.
4. Fare clic su **Sfoglia** e selezionare l'oggetto Criteri di dominio predefinito. Fare clic su **OK**.
5. Selezionare **Fine>Chiudi>OK**.
6. Espandere **Configurazione computer>Impostazioni di Windows>Impostazioni protezione>Criteri chiave pubblica**.
7. Fare clic con il pulsante destro del mouse su **Impostazioni richiesta automatica certificati** e selezionare **Nuovo>Richiesta automatica certificati**.
8. Fare clic su **Avanti** quando si avvia Installazione guidata richiesta automatica certificati.
9. Selezionare il modello **Controller di dominio** e fare clic su **Avanti**.
10. Selezionare l'autorità di certificazione elencata. Si tratta della stessa autorità di certificazione definita durante l'installazione di Servizi certificati. Fare clic su **Avanti**.
11. Fare clic su **Fine** per chiudere la procedura guidata.

Impostazione basata su browser senza schema

Tale impostazione può essere implementata mediante l'interfaccia di iLO 2 basata su browser.

1. Accedere a iLO 2 usando un account che dispone del privilegio Configure iLO 2 Settings (Configura impostazioni di iLO 2). Fare clic su **Administration** (Amministrazione).

   NOTA: Solo gli utenti che dispongono del privilegio Configure iLO 2 Settings (Configura impostazioni iLO 2) possono modificare queste impostazioni. Gli altri utenti potranno visualizzare solo le impostazioni assegnate.

2. Fare clic su **Directory Settings** (Impostazioni di directory).
3. Selezionare **Use Directory Default Schema** (Utilizza schema di directory predefinito) nella sezione Authentication Settings (Impostazioni autenticazione). Per ulteriori informazioni, vedere la sezione "Opzioni di impostazione senza schema" (Opzioni per l'impostazione senza schema a pagina 151).
4. Fare clic su **Apply Settings** (Applica impostazioni).
5. Fare clic su **Test Settings** (Verifica impostazioni).

Configurazione senza schema tramite script

Per configurare le directory senza schema mediante lo script RIBCL XML:

1. Scaricare e consultare la guida delle risorse mediante la riga di comando e lo scripting.
2. Scrivere uno script che configura iLO 2 per directory senza schema ed eseguirlo. È possibile utilizzare come modello il seguente script.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admin" PASSWORD="password">
<DIR_INFO MODE = "write">
<MOD_DIR_CONFIG>
<DIR_ENABLE_GRP_ACCT value = "yes"/>
<DIR_GRPACCT1_NAME value ="CN=Administrators,
CN=Builtin,DC=HP,DC=com "/>
<DIR_GRPACCT1_PRIV value = "1"/>
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

Impostazione senza schema basata su HPLOMIG

HPLOMIG rappresenta l'opzione più semplice per configurare un gran numero di processori LOM per le directory. Per utilizzare HPLOMIG, scaricare l'utility HPQLOMIG e la documentazione aggiuntiva dal sito Web HP (http://www.hp.com/servers/lights-out). HP raccomanda di utilizzare HPLOMIG quando si configura un gran numero di processori LOM per le directory. Per ulteriori informazioni sull'utilizzo di HPLOMIG, vedere "Utility di migrazione delle directory HPQLOMIG (Utility di migrazione delle directory HPQLOMIG a pagina 187)".

Opzioni per l'impostazione senza schema

Le opzioni di impostazione rimangono le stesse a prescindere da quale metodo (browser, HPQLOMIG o script) venga utilizzato per configurare la directory.

Dopo aver abilitato le directory e selezionato l'opzione senza schema, sono disponibili le seguenti opzioni:

Minima flessibilità di accesso

- Immettere il nome DNS del server di directory o l'indirizzo IP e la porta LDAP. Di solito, la porta LDAP di un collegamento SSL è 636.
- Immettere il nome distinto di almeno un gruppo. Può trattarsi di un gruppo di protezione, ad esempio: "CN=Administrators, CN=Builtin, DC=HP e DC=com" o di qualsiasi altro gruppo, fin quando gli utenti iLO 2 siano membri del gruppo.

  Con una configurazione minima, è possibile accedere a iLO 2 utilizzando il nome distinto completo e la password. È necessario essere membri di un gruppo riconosciuto da iLO 2.

Migliore flessibilità di accesso

- Oltre alle impostazioni minime, immettere almeno un contesto utente di directory.

  Al momento dell'accesso il nome di accesso e il contesto utente vengono combinati per formare il nome utente distinto. Ad esempio, se l'utente effettua l'accesso come "JOHN.SMITH" e viene impostato un contesto utente "CN=USERS,DC=HP,DC=COM", il nome distinto che iLO 2 tenterà sarà "CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM."

Massima flessibilità di accesso

- Configurare iLO 2 come descritto in precedenza.
- Configurare iLO 2 con un nome DNS, non un indirizzo IP per l'indirizzo di rete del server di directory. Il nome DNS deve essere risolvibile in un indirizzo IP valido per iLO 2 e il sistema client.
- Abilitare i controlli ActiveX nel browser. Lo script di accesso a iLO 2 tenterà di chiamare un controllo di Windows® per convertire il nome di accesso in un nome distinto.

  Configurare iLO 2 con la massima flessibilità di accesso consente un accesso mediante il nome distinto completo e una password, il nome come viene visualizzato nella directory, il formato NetBIOS (dominio/nome di accesso) oppure il formato di posta elettronica (login_name@domain).

NOTA: È possibile che le impostazioni di protezione del sistema o il software installato impediscano allo script di accesso di chiamare il controllo ActiveX di Windows®. Se ciò accade, il browser visualizzerà un messaggio di avviso nella barra di stato, una finestra di messaggio o potrebbe cessare di rispondere. Per individuare quale impostazione o software causino il problema, creare un altro profilo e accedere al sistema.

In alcuni casi, può non essere possibile far funzionare l'opzione relativa alla massima flessibilità di accesso. Ad esempio, se il client e iLO 2 si trovano in domini DNS diversi, uno dei due può non essere in grado di risolvere il nome del server di directory in un indirizzo IP.

Gruppi nidificati senza schema

In molte aziende gli utenti e gli amministratori sono strutturati in gruppi. In molti casi, può risultare utile mantenere questa organizzazione e associare i gruppi esistenti a uno o più oggetti ruolo di gestione di Integrated Lights-Out. Quando i dispositivi sono associati agli oggetti ruolo, infatti, l'amministratore può controllare l'accesso ai dispositivi Lights-Out associati al ruolo aggiungendo o eliminando membri dai gruppi.

Se si utilizza Microsoft® Active Directory, è possibile inserire un gruppo all'interno dell'altro in modo da creare un gruppo nidificato. Gli oggetti ruolo sono considerati gruppi e possono contenere altri gruppi al loro interno. È possibile aggiungere direttamente il gruppo nidificato esistente al ruolo e assegnare i diritti e le restrizioni appropriate. È possibile aggiungere nuovi utenti al gruppo esistente o al ruolo.

Nelle implementazioni precedenti, l'accesso a iLO 2 era consentito solo agli utenti senza schema membri diretti del gruppo principale. Se si utilizza l'integrazione senza schema, anche gli utenti che sono membri indiretti (ovvero membri di un gruppo nidificato del gruppo principale) possono accedere a iLO 2.

Novell eDirectory non consente l'uso di gruppi nidificati. Con eDirectory, gli utenti abilitati alla lettura di un ruolo sono considerati membri di tale ruolo. Quando si aggiunge un gruppo esistente, un'unità organizzativa o un'organizzazione a un ruolo, aggiungere l'oggetto come trustee di lettura del ruolo. Tutti i membri dell'oggetto sono considerati membri del ruolo. È possibile aggiungere nuovi utenti all'oggetto esistente o al ruolo.

Se per estendere il gruppo del ruolo si utilizzano le assegnazioni dei diritti di directory o di trustee, è necessario che gli utenti siano in grado di leggere l'oggetto LOM che rappresenta il dispositivo LOM. Per l'autenticazione degli utenti, alcuni ambienti richiedono che lo stesso trustee del ruolo venga letto come trustee dell'oggetto LOM.

Impostazione dell'integrazione di directory mediante lo schema HP

Se si utilizza l'integrazione delle directory mediante lo schema HP, iLO 2 supporta sia Active Directory che eDirectory. Tuttavia, questi servizi di directory richiedono l'estensione del suddetto schema.

Funzioni supportate dall'integrazione di directory mediante lo schema HP

Le funzionalità dei servizi di directory per iLO 2 consentono all'utente di:

- Autenticare gli utenti da un database utente condiviso, consolidato e scalabile.
- Controllare i privilegi dell'utente (autorizzazione) utilizzando il servizio di directory.
- Utilizzare i ruoli nel servizio di directory per l'amministrazione a livello di gruppo dei processori di gestione iLO 2 e degli utenti di iLO 2.

L'estensione dello schema deve essere eseguita dall'amministratore dello schema. Il database dell'utente locale viene conservato. L'utente può decidere di non utilizzare le directory, di utilizzare una combinazione di directory e di account locali o di utilizzare le directory solo per l'autenticazione.

NOTA: Il server di directory non è disponibile quando è collegato tramite la porta di diagnostica. È possibile accedere solo utilizzando un account locale.

Impostazione di servizi di directory

Per abilitare la gestione abilitata alle directory sui processori di gestione Lights-Out, procedere come segue:

1. Pianificazione

Vedere le seguenti sezioni:

- "Servizi di directory" (Servizi di directory a pagina 145)
- "Schema dei servizi di directory" (Schema dei servizi di directory a pagina 233)
- "Gestione remota abilitata alle directory" (Schema dei servizi di directory a pagina 233)

2. Installazione

   a. Scaricare il pacchetto HP Lights-Out Directory contenente il programma di installazione dello schema, il programma di installazione dello snap-in di gestione e le utility di migrazione dal sito Web HP (http://www.hp.com/servers/lights-out).

   b. Eseguire il programma di installazione dello schema (Programma di installazione dello schema a pagina 156) una volta per estendere lo schema

   c. Eseguire il programma di installazione dello snap-in di gestione (Programma di installazione degli snap-in di gestione a pagina 158) e installare lo snap-in appropriato per il servizio di directory utilizzato su una o più workstation di gestione.

3. Aggiornamento

   a. Eseguire l'aggiornamento della ROM sul processore di gestione Lights-Out con il firmware abilitato alla directory.

   b. Definire le impostazioni del server di directory e il nome distinto degli oggetti del processore di gestione nella pagina Directory Settings (Impostazioni di directory) (Impostazioni di directory a pagina 50) dell'interfaccia grafica di iLO 2.

4. Gestione

   a. Creare un oggetto periferica di gestione e un oggetto ruolo (Oggetti dei servizi di directory a pagina 165) utilizzando lo snap-in.

   b. Assegnare diritti all'oggetto ruolo, se necessario, e associare il ruolo all'oggetto dispositivo di gestione.

   c. Aggiungere utenti all'oggetto ruolo.

   Per ulteriori informazioni sulla gestione del servizio di directory, vedere la sezione "Gestione remota abilitata alle directory" (Gestione remota abilitata alla directory a pagina 179). Nelle sezioni "Servizi di directory per Active Directory " (Servizi di directory per Active Directory a pagina 158) e "Servizi di directory per eDirectory" (Servizi di directory per eDirectory a pagina 169) sono riportati alcuni esempi.

5. Gestione delle eccezioni

   - Le utility di migrazione di Lights-Out sono più facili da utilizzare con un unico ruolo Lights-Out. Se si prevede di creare più ruoli nella directory, è consigliabile avvalersi di utility di script delle directory quali script LDIFDE o VB, che consentono di creare associazioni di ruoli complesse. Per ulteriori informazioni, vedere la sezione "Utilizzo degli strumenti di importazione principali" (Utilizzo degli strumenti di importazione principali a pagina 185).

   - Se si dispone di processori iLO 2 o RILOE con firmware meno recente, può essere necessario aggiornarli manualmente tramite il browser. Di seguito sono riportati i requisiti minimi di firmware per l'aggiornamento remoto del firmware tramite RIBCL e l'utility di migrazione delle directory:

Prodotto LOM	Firmware minimo supportato
RILOE	2.41

Prodotto LOM	Firmware minimo supportato
RILOE II	Tutte le versioni
iLO (Porta: iLO)	1.4x
iLO 2	1.1x

Dopo avere esteso lo schema, è possibile completare l'impostazione dei servizi di directory tramite le utility di migrazione delle directory di Lights-Out HP (Utility di migrazione delle directory HPQLOMIG a pagina 187). Le utility di migrazione sono incluse nel pacchetto HP Lights-Out Directory. La versione 1.13 dell'utility di migrazione delle directory consente a Lights-Out di importare, esportare e supportare diverse credenziali utente per ogni processore Lights-Out.

Documentazione dello schema

Per semplificare il processo di pianificazione e approvazione, HP fornisce una documentazione relativa alle modifiche apportate allo schema durante la procedura di configurazione dello schema stesso. Per una verifica delle modifiche apportate allo schema esistente, vedere la sezione "Schema dei servizi di directory" (Schema dei servizi di directory a pagina 233).

Supporto dei servizi di directory

Se si utilizza l'integrazione delle directory mediante lo schema HP, iLO 2 supporta i seguenti servizi di directory:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Microsoft® Windows® Server 2008 Active Directory
- Novell eDirectory 8.7.3
- Novell eDirectory 8.7.1

Il software iLO 2 è progettato per funzionare con Utenti e computer di Microsoft® Active Directory e con gli strumenti di gestione Novell ConsoleOne, che permettono di gestire gli account utente su Microsoft Active Directory o Novell eDirectory. Questa soluzione non fa distinzione tra eDirectory eseguita su NetWare, Linux, o Windows®. La creazione dell'estensione di uno schema eDirectory richiede Java 1.4.0 o versione successiva per l'autenticazione SSL.

iLO 2 supporta Microsoft® Active Directory su uno dei seguenti sistemi operativi:

- Windows Server® 2008
- Windows Server® 2003

iLO 2 supporta eDirectory su sistema operativo Novell.

Software richiesto per lo schema

iLO 2 richiede un software specifico per l'espansione dello schema e fornisce gli snap-in per la gestione della rete iLO 2. È possibile scaricare un componente HP Smart che contiene il programma di installazione dello schema e quello dello snap-in di gestione. Per scaricare il componente HP Smart, accedere al sito Web HP (http://www.hp.com/servers/lights-out).

Non è possibile eseguire il programma di installazione dello schema sul controller di dominio in cui si trova Windows Server® 2008 Core. Per motivi di sicurezza e di prestazioni, infatti, Windows Server® 2008 Core non utilizza un'interfaccia utente. Per eseguire il programma di installazione dello schema,

è necessario installare prima un'interfaccia utente sul controller di dominio oppure utilizzare un controller di dominio in cui si trovi una versione precedente di Windows®.

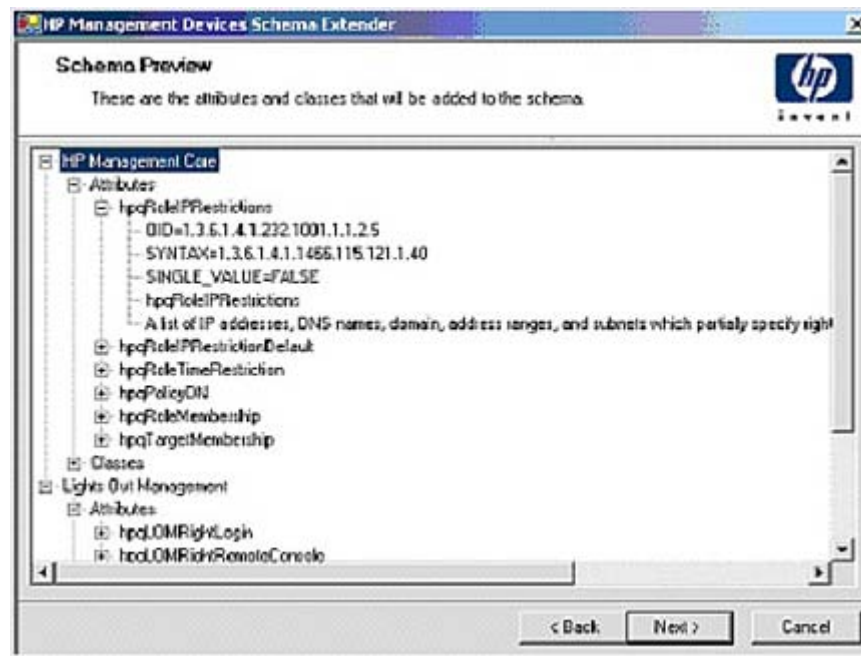
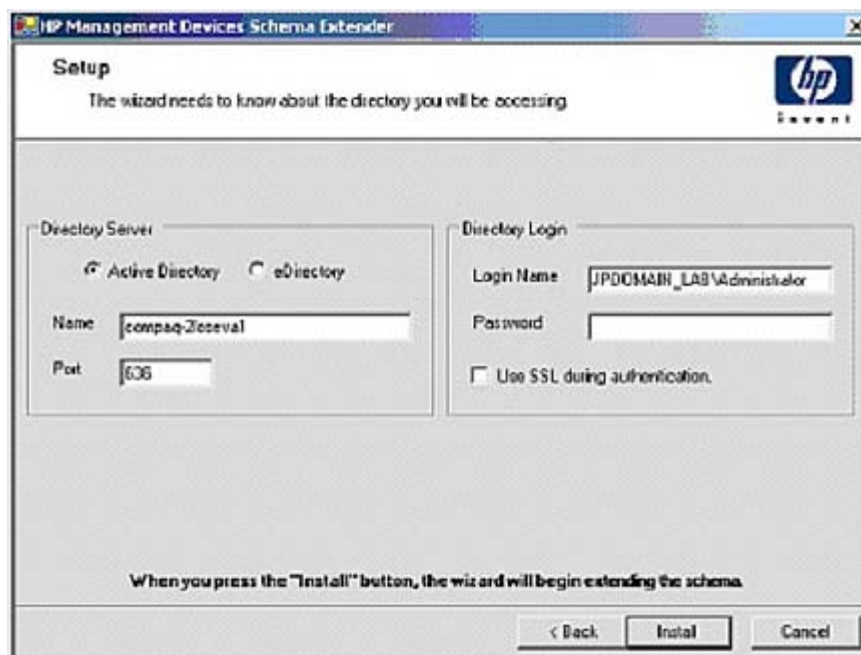
Programma di installazione dello schema

Insieme al programma di installazione dello schema vengono forniti uno o più file .xml. Questi file contengono lo schema che sarà aggiunto alla directory. In genere, uno di questi file conterrà lo schema centrale comune a tutti i servizi di directory supportati. I file supplementari contengono solo schemi specifici del prodotto. Il programma di installazione dello schema richiede l'uso di .NET Framework.

Il programma di installazione include tre importanti schermate:

- Schema Preview
- Setup
- Results

Schema Preview

La schermata Schema Preview consente all'utente di visualizzare le proposte di estensione dello schema. Questa schermata legge i file dello schema selezionati, esamina l'XML e lo visualizza come vista a struttura gerarchica. Elenca tutti i dettagli degli attributi e delle classi che verranno installati.

Setup

La schermata Setup (Installazione) consente di immettere le informazioni appropriate prima di eseguire l'estensione dello schema.

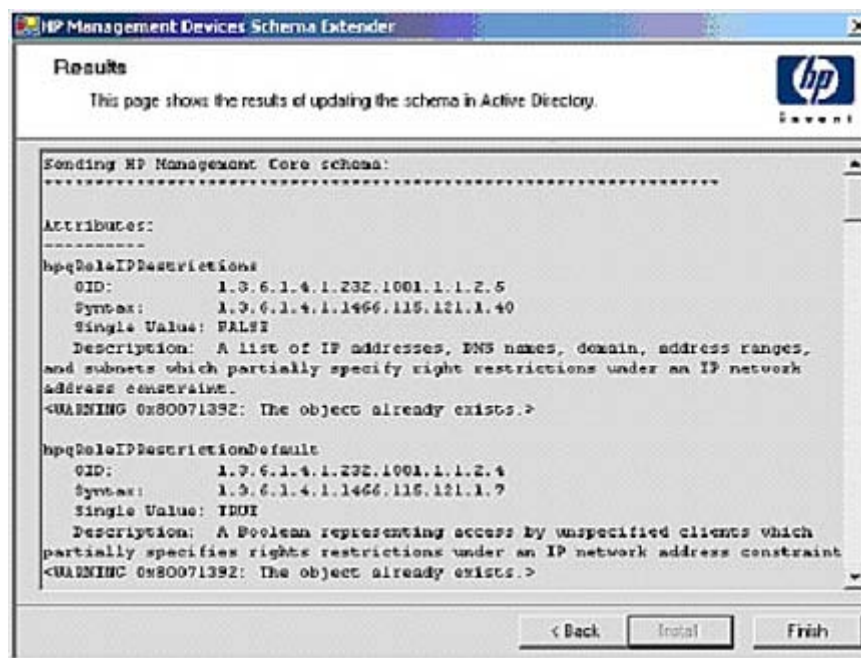
La sezione Directory Server (Server di directory) della schermata consente di stabilire se si utilizzerà Active Directory o eDirectory e di impostare il nome del computer e la porta di comunicazione LDAP.

NOTA: L'estensione dello schema sul servizio Active Directory richiede che l'utente sia un amministratore dello schema autenticato, che lo schema non sia protetto dalla scrittura e che la directory sia il proprietario del ruolo FSMO nella struttura. Il programma di installazione cerca di rendere il server di directory di destinazione il master dello schema FSMO.

Per ottenere l'accesso di scrittura allo schema su Windows® 2000, è necessario cambiare il blocco di sicurezza del registro. Se l'utente seleziona l'opzione **Active Directory**, il programma di estensione dello schema tenta di modificare il registro. Ciò è possibile solo se l'utente possiede i diritti necessari. L'accesso in scrittura allo schema è abilitato automaticamente su Windows® Server 2003.

La sezione Directory Login (Login alla directory) della schermata Setup (Installazione) consente di immettere il nome di accesso e la password. Per completare l'estensione dello schema, potrebbero essere richiesti questi dati. L'opzione Use SSL during authentication (Usa SSL durante l'autenticazione) imposta la forma di autenticazione sicura da utilizzare. Se questa opzione è selezionata, viene utilizzata l'autenticazione di directory SSL. Se questa opzione non è selezionata ed è selezionato il servizio Active Directory, verrà utilizzata l'autenticazione di Windows NT®. Se questa opzione non è selezionata ed è selezionato il servizio eDirectory, l'autenticazione dell'amministratore e l'estensione dello schema verranno eseguite utilizzando una connessione non criptata (testo normale).

Results

La schermata Results (Risultati) visualizza i risultati dell'installazione, inclusa la possibilità di estensione dello schema e gli attributi modificati in precedenza.

Programma di installazione degli snap-in di gestione

Il programma di installazione dello snap-in di gestione è necessario per gestire gli oggetti iLO 2 in una directory Utenti e computer di Microsoft® Active Directory o in una directory Novell ConsoleOne.

Gli snap-in iLO 2 vengono utilizzati per eseguire le seguenti operazioni nella creazione di una directory iLO:

- Creazione e gestione di oggetti iLO 2 e di oggetti ruolo (gli oggetti criteri saranno supportati nelle versioni future).
- Creazione delle associazioni tra oggetti iLO 2 e oggetti ruolo (o oggetti criteri).

Servizi di directory per Active Directory

Le sezioni seguenti descrivono i prerequisiti di installazione, la preparazione e un esempio pratico dei servizi di directory per Active Directory. HP fornisce una utility che consente di automatizzare gran parte della procedura di configurazione delle directory. Per scaricare l'utility HP Directories Support for Management Processors (Supporto delle directory HP per processori di gestione), visitare il sito Web HP (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Prerequisiti di installazione per Active Directory

- Affinché iLO 2 possa collegarsi in modo sicuro sulla rete, Active Directory deve disporre di un certificato digitale installato.
- Active Directory deve avere uno schema esteso che descriva le classi di oggetto e le proprietà di Lights-Out.
- La versione del firmware deve essere iLO v1.40 o successiva oppure iLO v1.00 o successiva.
- È necessaria la licenza per usufruire delle funzionalità di iLO 2 Advanced.

  È possibile eseguire una copia di valutazione di iLO Advanced utilizzando una chiave di licenza gratuita scaricabile dal sito Web HP (http://h10018.www1.hp.com/wwsolutions/iLO/iLOeval.html).

I servizi di directory per iLO 2 utilizzano LDAP su SSL per comunicare con i server di directory. Prima di installare gli snap-in e lo schema per Active Directory, leggere e tenere a disposizione la seguente documentazione:

NOTA: L'installazione dei servizi di directory per iLO 2 richiede l'estensione dello schema di Active Directory. L'estensione dello schema deve essere completato da un amministratore dello schema di Active Directory.

- *Extending the Schema* (Estensione dello schema) nel Server Resource Kit di Microsoft® Windows® 2000, disponibile sul sito Web Microsoft® (http://msdn.microsoft.com).
- *Installing Active Directory* (Installazione di Active Directory) nel Server Resource Kit di Microsoft® Windows® 2000.
- Articoli della Knowledge Base Microsoft®.

  Per accedere a questi articoli, utilizzare l'opzione di ricerca nella Knowledge Base basata sul numero ID dell'articolo, disponibile sul sito Web Microsoft® (http://support.microsoft.com/).

  - 216999 *Installing the Remote Server Administration Tools in Windows® 2000 (Installazione degli strumenti di amministrazione dei server remoti in Windows® 2000)*
  - 314978 *Using the Adminpak.msi to Install a Server Administration Tool in Windows® 2000 (Uso di Adminpak.msi per installare uno strumento di amministrazione del server in Windows® 2000)*
  - 247078 *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers (Abilitazione della comunicazione SSL tramite LDAP per i controller di dominio Windows® 2000)*
  - 321051 *Enabling LDAP over SSL with a Third-Party Certificate Authority (Abilitazione di LDAP su SSL con un'autorithy di certificazione esterna)*
  - 299687 *MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed (Le funzioni esposte dall'uso di LDAP su SSL possono abilitare la modifica delle password)*

Per comunicare con il servizio di directory, iLO 2 richiede una connessione sicura. A tal fine, è necessario eseguire l'installazione dell'autorità di certificazione Microsoft®. Per informazioni tecniche, consultare l'articolo della Knowledge Base Microsoft® 321051: *How to Enable LDAP over SSL with a Third-Party Certification Authority (Come abilitare LDAP su SSL con un'authority di certificazione esterna).*

Installazione di Active Directory su Windows Server 2008

Per lo schema predefinito:

1. Disabilitare IPV6 e installare Active Directory, il servizio DNS e la CA principale in Windows Server® 2008.
2. Eseguire l'accesso a iLO e andare alla pagina Directory Settings (Impostazioni di directory). Fare clic su **Administration>Security>Directory** (Amministrazione>Protezione>Directory).
3. Nella pagina Directory Settings (Impostazioni di directory) immettere le impostazioni relative alla directory.
4. In Directory User Context (Contesto utente di directory) immettere le impostazioni relative alla directory.

5. Creare Administer Groups (Amministra gruppi) per gli utenti iLO.
6. Fare clic su **Administration>Network>DHCP/DNS** (Amministrazione>Rete>DHCP/DNS) e nei campi Domain Name (Nome dominio) e Primary DNS server (Server DNS primario) modificare le impostazioni relative all'ambiente.

Per lo schema esteso:

1. Disabilitare IPV6 e installare Active Directory, il servizio DNS e la CA principale in Windows Server® 2008.
2. The iLO LDAP Component (Componente LDAP iLO) richiede .Net Framework 1.1_4322. Installare .Net Framework.
3. Installare la versione più recente del componente LDAP iLO (sp31581 o successiva).
4. Estendere lo schema utilizzando HP Management Devices Schema Extender (Utility di estensione dello schema dei dispositivi di gestione HP).
5. Installare lo snap-in del componente LDAP HP.
6. Creare HP Device (Dispositivo HP) e HP Role (Ruolo HP).
7. Eseguire l'accesso a iLO e andare alla pagina Directory Settings (Impostazioni di directory). Fare clic su **Administration>Security>Directory** (Amministrazione>Protezione>Directory).
8. Immettere le impostazioni relative alla propria directory.
9. Immettere il contesto dell'utente di directory.
10. Fare clic su **Administration>Network>DHCP/DNS** (Amministrazione>Rete>DHCP/DNS) e nei campi Domain Name (Nome dominio) e Primary DNS server (Server DNS primario) modificare le impostazioni relative all'ambiente.

Il componente LDAP non può essere utilizzato con un'installazione core di Windows Server® 2008.

Preparazione dei servizi di directory per Active Directory

Per installare i servizi di directory in modo da poter essere utilizzati con i processori di gestione iLO 2:

1. Installare Active Directory. Per ulteriori informazioni, consultare il documento *Installing Active Directory* (Come installare Active Directory) nel Server Resource Kit di Microsoft® Windows® 2000.
2. Installare Microsoft® Admin Pack (il file ADMINPAK.MSI che si trova nella sottodirectory i386 del CD di Windows® 2000 Server o Advanced Server). Per ulteriori informazioni, consultare l'articolo della Knowledge Base Microsoft® 216999.
3. In Windows® 2000, il blocco di sicurezza che impedisce la scrittura accidentale sullo schema deve essere temporaneamente disabilitato. L'utility di estensione dello schema può eseguire questa operazione se il servizio di registro remoto è attivo e l'utente dispone dei diritti sufficienti. Questa operazione può essere anche eseguita impostando `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\ServicesParameters\Schema Update Allowed` nel registro di sistema su un valore diverso da zero (vedere la sezione "Order of Processing When Extending the Schema" (Ordine di elaborazione nell'estensione dello schema) nel documento *Installation of Schema Extensions* (Installazione delle estensioni dello schema) incluso nel Resource Kit di Windows® 2000 Server) o procedendo come descritto di seguito. Questo passaggio non è necessario se si utilizza Windows® Server 2003.

NOTA: La modifica errata del registro può danneggiare seriamente il sistema. HP raccomanda di creare una copia di backup dei dati importanti sul computer prima di apportare modifiche al registro.

a. Avviare MMC.

b. Installare lo snap-in dello schema di Active Directory in MMC.

c. Fare clic con il pulsante destro del mouse su **Active Directory Schema** (Schema di Active Directory) e selezionare **Operations Master** (Master operazioni).

d. Selezionare **The Schema may be modified on this Domain Controller** (Lo schema su questo controller di dominio può essere modificato).

e. Fare clic su **OK**.

   Potrebbe essere necessario espandere la cartella Schema di Active Directory per rendere disponibile la casella di controllo.

4. Creare un certificato o installare Servizi certificati. Questo passaggio è necessario per creare un certificato o installare Servizi certificati, poiché la comunicazione di iLO 2 con Active Directory avviene tramite SSL. Prima di installare Servizi certificati, installare Active Directory.

5. Per specificare che un certificato deve essere rilasciato al server che esegue Active Directory:

   a. Avviare Microsoft Management Console sul server e aggiungere lo snap-in del criterio del dominio predefinito (Criterio di gruppo, quindi selezionare l'oggetto criterio dominio predefinito).

   b. Fare clic su **Configurazione computer>Impostazioni di Windows>Impostazioni protezione>Criteri chiave pubblica**.

   c. Fare clic con il pulsante destro del mouse su **Impostazioni richiesta automatica certificati** e selezionare **Nuovo>Richiesta automatica certificati**.

   d. Utilizzando la procedura guidata, selezionare il modello di controller del dominio e l'autorità di certificazione che si desidera utilizzare.

6. Scaricare il componente Smart che contiene i programmi di installazione per l'estensione dello schema e gli snap-in. Per scaricare il componente Smart, visitare il sito Web HP (http://www.hp.com/servers/lights-out).

7. Eseguire il programma di installazione dello schema che estende lo schema di directory con gli oggetti HP appropriati.

   Il programma di installazione dello schema associa gli snap-in di Active Directory al nuovo schema. L'utility di installazione degli snap-in è uno script di installazione Windows® MSI e può essere utilizzato su tutti i sistemi operativi che supportano MSI (Windows® XP, Windows® 2000, Windows® 98). Alcune parti dell'estensione dello schema richiedono tuttavia .NET Framework, che può essere scaricato dal sito Web Microsoft® (http://www.microsoft.com).

Installazione e inizializzazione degli snap-in per Active Directory

1. Eseguire il programma di installazione per installare gli snap-in.
2. Configurare il servizio di directory per disporre delle relazioni e degli oggetti appropriati per la gestione di iLO 2.
   a. Utilizzare gli snap-in di gestione HP per creare gli oggetti iLO 2, Criteri, Amministrazione e Ruolo utente.
   b. Utilizzare gli snap-in di gestione HP per creare le associazioni tra l'oggetto iLO 2, l'oggetto criteri e l'oggetto ruolo.
   c. Puntare l'oggetto iLO 2 sugli oggetti Amministratore e Ruolo utente (questi punteranno di nuovo automaticamente sull'oggetto iLO 2).

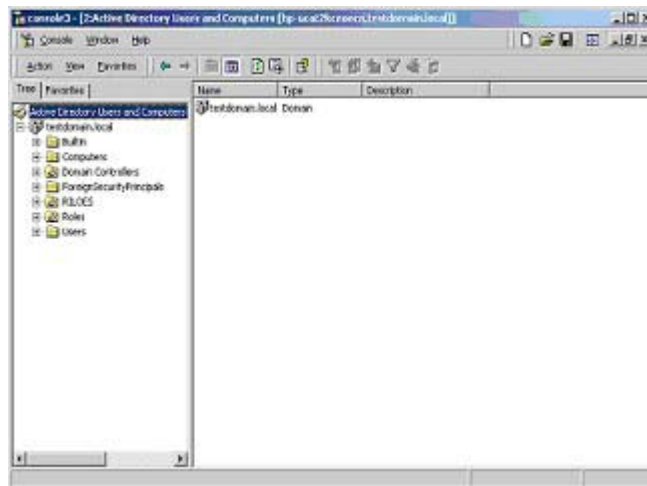
      Per ulteriori informazioni sugli oggetti iLO 2, vedere la sezione "Oggetti dei servizi di directory" (Oggetti dei servizi di directory a pagina 165).

È necessario creare come minimo:

- Un oggetto Ruolo che conterrà uno o più utenti e uno o più oggetti iLO 2.
- Un oggetto iLO 2 corrispondente a ciascun processore di gestione iLO 2 che utilizzerà la directory.

Esempio: Creazione e configurazione degli oggetti di directory per l'uso con iLO 2 in Active Directory

L'esempio seguente spiega come impostare i ruoli e i dispositivi HP in una directory aziendale con il dominio *testdomain.local*, costituito da due unità organizzative: *Roles* e *RiLOES*.

Supponiamo che un'azienda disponga di una directory aziendale che includa il dominio *testdomain.local* strutturato come riportato nella seguente schermata.

Creare un'unità organizzativa che conterrà i dispositivi Lights-Out gestiti dal dominio. In questo esempio, si creano due unità organizzative denominate *Roles* e *RiLOES*.

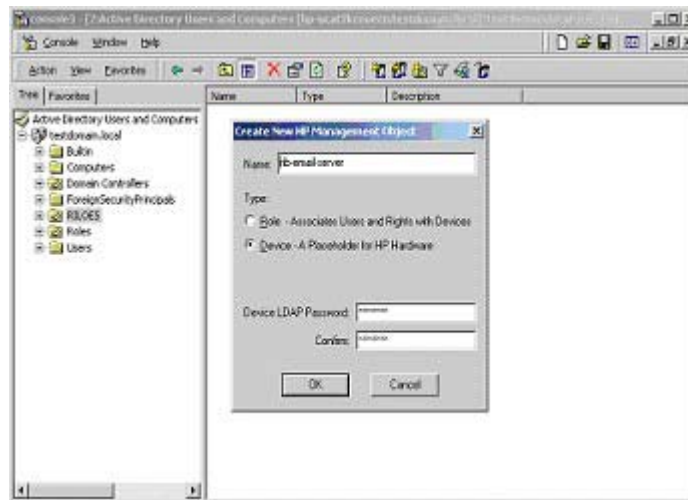
1. Utilizzare gli snap-in di Utenti e computer di Active Directory forniti da HP per creare oggetti di gestione Lights-Out nell'unità organizzativa *RiLOES* per vari dispositivi iLO 2.

   a. Fare clic con il pulsante destro del mouse sull'unità organizzativa RiLOES che si trova nel dominio *testdomain.local*, quindi selezionare **NewHPObject**.

   b. Nella finestra di dialogo Create New HP Management Object (Crea nuovo oggetto di gestione HP), selezionare **Device** (Dispositivo).

   c. Immettere un nome appropriato nel campo Name (Nome) della finestra di dialogo. In questo esempio, il nome host DNS di iLO 2, *rib-email-server*, sarà utilizzato come nome dell'oggetto di gestione di Lights-Out, e il cognome sarà *RiLOEII*.

      Immettere e confermare una password nei campi Device LDAP Password (Password dispositivo LDAP) e Confirm (Conferma). Il dispositivo utilizzerà questa password, che deve essere univoca per il dispositivo, per l'autenticazione della directory. Questa è la password utilizzata nella schermata Directory Settings (Impostazioni di directory) di iLO 2.

   d. Fare clic su **OK**.

2. Utilizzare gli snap-in di utenti e computer Active Directory forniti da HP per creare oggetti ruolo HP nell'unità organizzativa *Roles*.

   a. Fare clic con il pulsante destro del mouse sull'unità organizzativa Roles (Ruoli), selezionare **New** (Nuovo) quindi **Object** (Oggetto).

   b. Selezionare **Role** (Ruolo) come tipo di campo nella finestra di dialogo Create New HP Management Object (Crea nuovo oggetto di gestione HP).

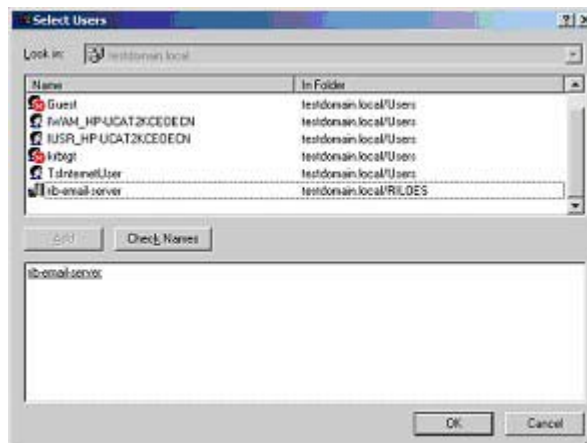
   c. Immettere un nome appropriato nel campo Name (Nome) nella finestra di dialogo New HP Management Object (Nuovo oggetto di gestione HP). In questo esempio, il ruolo conterrà utenti qualificati per l'amministrazione del server remoto e si chiamerà *remoteAdmins*. Fare clic su **OK**.

   d. Ripetere il processo creando un ruolo per i monitor dei server remoti denominato *remoteMonitors*.

3. Utilizzare gli snap-in per gli utenti e i computer Active Directory di HP per assegnare i diritti ai ruoli e associare i ruoli a utenti e dispositivi.

   a. Fare clic con il pulsante destro del mouse su **remoteAdmins** nell'unità organizzativa Roles del dominio *testdomain.local* e selezionare **Properties** (Proprietà)

   b. Selezionare la scheda **HP Devices** (Dispositivi HP), quindi fare clic su **Add** (Aggiungi).

   c. Utilizzando la finestra di dialogo Select Users (Seleziona utenti), selezionare l'oggetto di gestione di Lights-Out creato al passaggio 2, *rib-email-server* nella cartella testdomain.local/RiLOES. Fare clic su **OK** per chiudere la finestra di dialogo, quindi su **Apply** (Applica) per salvare l'elenco.

   d. Aggiungere gli utenti al ruolo. Fare clic sulla scheda **Members** (Membri) e aggiungere gli utenti utilizzando il pulsante Add (Aggiungi) e la finestra di dialogo Select Users (Seleziona utenti). I dispositivi e gli utenti ora sono associati.

4. Utilizzare la scheda Lights Out Management (Gestione di Lights Out) per impostare i diritti per il ruolo. Tutti gli utenti e i gruppi all'interno di un ruolo hanno i diritti assegnati al ruolo su tutti i dispositivi iLO 2 gestiti dal ruolo stesso. In questo esempio, gli utenti del ruolo *remoteAdmins*

avranno accesso completo alle funzionalità di iLO 2. Selezionare le caselle accanto a ciascun diritto, quindi fare clic su **Apply** (Applica). Fare clic su **OK** per chiudere il foglio delle proprietà.

5. Utilizzando la stessa procedura descritta al passaggio 4, modificare le proprietà del ruolo *remoteMonitors*, aggiungere il dispositivo *rib-email-server* all'elenco Managed Devices (Dispositivi gestiti) nella scheda HP Devices (Dispositivi HP) e aggiungere gli utenti al ruolo *remoteMonitors* utilizzando la scheda Members (Membri). Quindi, nella scheda Lights Out Management (Gestione di Lights Out), selezionare la casella accanto Login (Accesso). Fare clic su **Apply** (Applica), quindi su **OK**. I membri del ruolo *remoteMonitors* potranno autenticare e visualizzare lo stato del server.

I diritti utente per ciascun dispositivo iLO 2 consisteranno nella somma di tutti i diritti assegnati da tutti i ruoli nei quali l'utente è membro e in cui il dispositivo iLO 2 è un dispositivo gestito. Seguendo gli esempi precedenti, se un utente è presente nei ruoli *remoteAdmins* e *remoteMonitors* avrà tutti i diritti, poiché il ruolo *remoteAdmins* ha tali diritti.

Per configurare un dispositivo iLO 2 e associarlo all'oggetto di gestione Lights-Out riportato in questo esempio, utilizzare le impostazioni simili a quelle della seguente schermata Directory Settings (Impostazioni di directory).

```
RIB Object DN = cn=rib-email-server,ou=RILOES,dc=testdomain,dc=local
Directory User Context 1 = cn=Users,dc=testdomain,dc=local
```

Ad esempio, per ottenere l'accesso, l'utente *Mel Moore* con ID esclusivo *MooreM*, incluso nell'unità organizzativa degli utenti con il dominio *testdomain.local*, nonché membro del ruolo *remoteAdmins* o *remoteMonitors*, potrà accedere a iLO 2 immettendo `testdomain\moorem` o `moorem@testdomain.local` o `Mel Moore` nel campo Login Name (Nome di accesso) della schermata di accesso di iLO 2 e digitando la password di Active Directory nel campo Password.

Oggetti dei servizi di directory

Uno degli elementi principali della gestione basata su directory consiste nella corretta virtualizzazione dei servizi gestiti all'interno del servizio di directory. Questa virtualizzazione consente all'amministratore di creare relazioni tra il dispositivo gestito e l'utente o i gruppi già contenuti nel servizio di directory. La gestione utente di iLO 2 richiede la presenza di tre oggetti base nel servizio di directory:

- Oggetto di gestione di Lights-Out
- Oggetto ruolo
- Oggetto utente

Ciascun oggetto rappresenta un dispositivo, un utente o una relazione necessaria per la gestione basata su directory.

NOTA: Dopo aver installato gli snap-in, è necessario riavviare ConsoleOne e MMC per visualizzare le nuovi voci.

Una volta installato lo snap-in, sarà possibile creare gli oggetti iLO 2 e i ruoli iLO 2 all'interno della directory. Utilizzando lo strumento Utenti e Computer, l'utente sarà in grado di:

- Creare gli oggetti iLO 2 e ruolo.
- Aggiungere utenti agli oggetti ruolo.
- Impostare i diritti e le restrizioni degli oggetti ruolo.

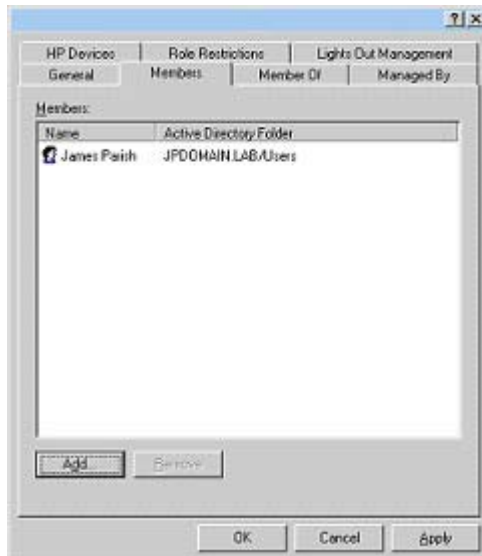
Snap-in di Active Directory

Le sezioni seguenti descrivono le opzioni di gestione supplementari disponibili nello strumento utenti e computer di Active Directory dopo l'installazione degli snap-in HP.

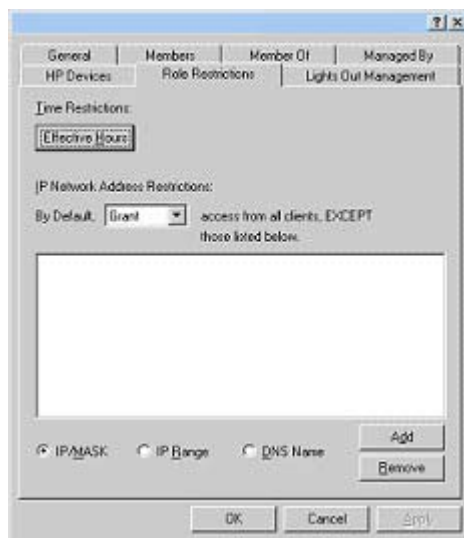
Dispositivi HP

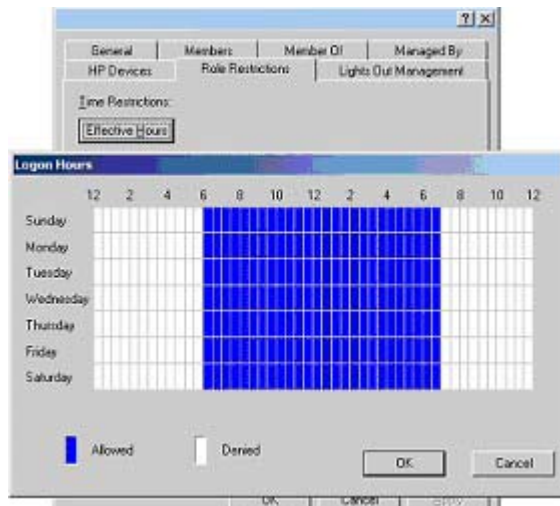
La scheda HP Devices (Dispositivi HP) consente di aggiungere i dispositivi HP da gestire all'interno di un ruolo. Facendo clic su **Add** (Aggiungi), è possibile visualizzare un dispositivo HP specifico e aggiungerlo all'elenco dei dispositivi membri. Facendo clic su **Remove** (Rimuovi), è possibile visualizzare un dispositivo HP specifico e rimuoverlo dall'elenco dei dispositivi membri.

Membri

Dopo aver creato gli oggetti utenti, la scheda Members (Membri) consente di gestire gli utenti all'interno del ruolo. Facendo clic su **Add** (Aggiungi), sarà possibile visualizzare l'utente specifico che si desidera aggiungere. Evidenziando un utente esistente e facendo clic su **Remove** (Rimuovi), l'utente verrà rimosso dall'elenco dei membri validi.

Restrizioni dei ruoli di Active Directory

La sottoscheda Role Restrictions (Restrizioni ruoli) consente di impostare le restrizioni di accesso per il ruolo. Queste restrizioni includono:

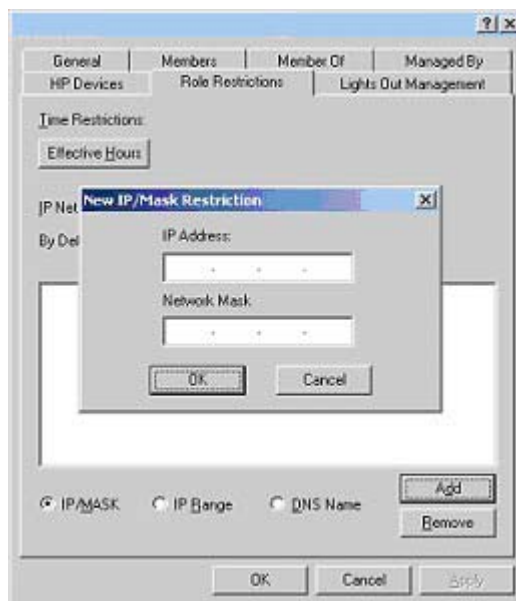
- Restrizioni temporali
- Restrizioni relative agli indirizzi IP di rete
  - IP/maschera
  - Intervallo IP
  - Nome DNS

Restrizioni temporali

Facendo clic su **Effective Hours** (Ore effettive) nella scheda Role Restrictions (Restrizioni ruolo), è possibile gestire le ore disponibili per l'accesso dei membri del ruolo. Nella finestra a comparsa Logon Hours (Ore di accesso), è possibile selezionare le ore disponibili per l'accesso in ciascun giorno della settimana a incrementi di 30 minuti. È possibile modificare un singolo quadrato facendo clic su di esso oppure modificare una sezione di quadrati facendo clic e tenendo premuto il pulsante del mouse, quindi trascinando il cursore sui quadrati da modificare e rilasciando infine il pulsante del mouse. L'impostazione predefinita consente l'accesso in qualunque momento.

Indirizzo IP client forzato o accesso al nome DNS

È possibile concedere o negare l'accesso a un indirizzo IP, a un intervallo di indirizzi IP o ai nomi DNS.

1. Nel menu a discesa By Default (Impostazione predefinita) selezionare **Grant** (Concedi) o **Deny** (Nega) per concedere o negare l'accesso da tutti gli indirizzi, ad eccezione degli indirizzi IP, degli intervalli di indirizzi IP e dei nomi DNS specificati.
2. Selezionare gli indirizzi da aggiungere, selezionare il tipo di restrizione e fare clic su **Add** (Aggiungi).
3. Immettere le informazioni nella finestra a comparsa relativa alle nuove restrizioni e fare clic su **OK**. Verrà visualizzata la finestra a comparsa relativa alle nuove restrizioni.

   L'opzione DNS Name (Nome DNS) consente di limitare l'accesso in base a un singolo nome DNS o a un sottodominio immesso nella forma host.azienda.com oppure *.dominio.azienda.com.
4. Fare clic su **OK** per salvare le modifiche.

Per rimuovere delle voci, evidenziarle nell'elenco visualizzato e fare clic su **Remove** (Rimuovi).

Gestione Lights-Out di Active Directory

Dopo aver creato un ruolo, è possibile selezionare i diritti da assegnarvi. Gli utenti e gli oggetti dei gruppi possono divenire membri del ruolo per consentire l'assegnazione dei diritti associati a un singolo utente o a gruppi di utenti. I diritti sono gestiti nella scheda Lights Out Management (Gestione Lights Out).

Sono disponibili i seguenti diritti:

- **Login** (Accesso) - Questa opzione controlla la possibilità di accesso degli utenti ai dispositivi associati.
- **Remote Console** (Console remota) - Questa opzione consente l'accesso dell'utente alla console remota.
- **Virtual Media** (Supporti virtuali) - Questa opzione consente all'utente di accedere alla funzionalità dei supporti virtuali di iLO.
- **Server Reset and Power** (Alimentazione e reimpostazione del server) – Questa opzione consente all'utente di accedere al pulsante Virtual Power (Accensione virtuale) di iLO 2 per la reimpostazione remota del server o per il relativo spegnimento.
- **Administer Local User Accounts** (Amministra account utente locale) - Questa opzione consente all'utente di amministrare gli account. L'utente può modificare le impostazioni del proprio account, modificare le impostazioni degli account di altri utenti e aggiungere o eliminare altri utenti.
- **Administer Local Device Settings** (Amministra impostazioni dispositivi locali) – Questa opzione consente all'utente di configurare le impostazioni del processore di gestione iLO 2. Queste impostazioni includono le opzioni disponibili nelle schermate Global Settings (Impostazioni globali), Network Settings (Impostazioni di rete), SNMP Settings (Impostazioni SNMP) e Directory Settings (Impostazioni di directory) del browser Web di iLO 2.

Servizi di directory per eDirectory

Le sezioni seguenti descrivono i prerequisiti di installazione, la preparazione e un esempio pratico dei servizi di directory per eDirectory.

Prerequisiti di installazione per eDirectory

I servizi di directory di iLO 2 utilizzano LDAP su SSL per comunicare con i server di directory. Il software iLO 2 è progettato per l'installazione in una struttura eDirectory versione 8.6.1 e successiva. HP

sconsiglia di installare questo prodotto se si dispone di server eDirectory con una versione inferiore a eDirectory 8.6.1. Prima di installare gli snap-in e le estensioni dello schema per eDirectory, leggere e tenere a disposizione i seguenti documenti tecnici, reperibili presso il supporto Novell (http://support.novell.com).

L'installazione dei servizi di directory per iLO 2 richiede l'estensione dello schema di directory. L'estensione dello schema deve essere eseguita dall'amministratore dello schema.

- TID10066591 *Novell eDirectory 8.6 NDS compatibility* (Compatibilità Novell eDirectory 8.6 NDS)
- TID10057565 *Unknown objects in a mixed environment* (Oggetti non noti in ambiente vario)
- TID10059954 *How to test whether LDAP is working correctly* (Come collaudare il funzionamento corretto di LDAP)
- TID10023209 *How to configure LDAP for SSL (secure) connections* (Come configurare LDAP per collegamenti SSL sicuri)
- TID10075010 *How to test LDAP authentication* (Come collaudare l'autenticazione LDAP)

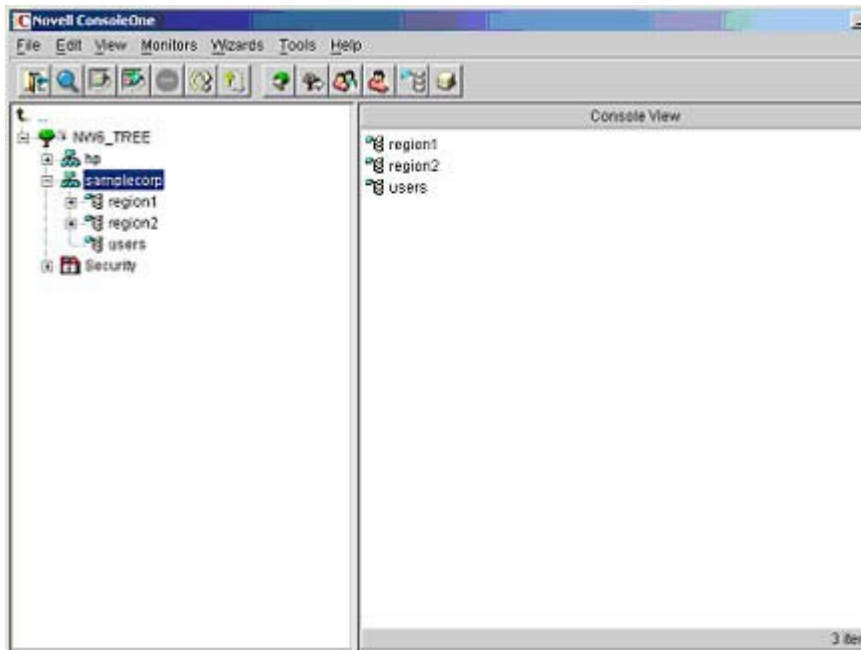
Installazione e inizializzazione degli snap-in per eDirectory

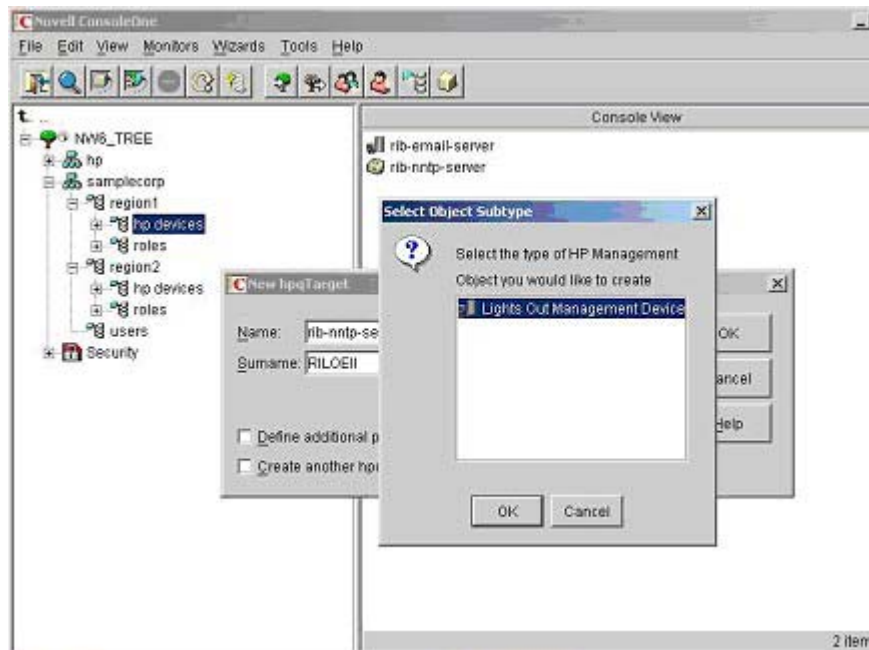
Per istruzioni dettagliate sull'uso dell'applicazione di installazione degli snap-in, vedere la sezione relativa all'installazione e all'inizializzazione degli snap-in (Installazione e inizializzazione degli snap-in per Active Directory a pagina 162).

NOTA: Dopo aver installato gli snap-in, è necessario riavviare ConsoleOne e MMC per visualizzare le nuovi voci.

Esempio: Creazione e configurazione degli oggetti di directory per l'uso con dispositivi LOM in eDirectory

L'esempio seguente illustra come configurare i ruoli e le periferiche HP in una società denominata *samplecorp*, costituita da due regioni, *region1* e *region2*.

Supponiamo che *samplecorp* sia una directory aziendale organizzata in base alla seguente schermata.

1. Creare unità organizzative in ciascuna regione. Ogni unità organizzativa dovrà contenere dispositivi LOM e ruoli specifici per la regione di appartenenza. In questo esempio vengono create due unità organizzative, denominate "*roles*" e "*hp devices*", in ciascuna unità organizzativa: "*region1*" e "*region2*".
2. Utilizzando gli snap-in di ConsoleOne forniti da HP, creare oggetti di gestione Lights-Out nelle unità organizzative *hp devices* per più dispositivi iLO 2.
   - **a.** Fare clic con il pulsante destro del mouse sull'unità organizzativa **hp devices** nell'unità organizzativa *region1* e selezionare **New**>**Object** (Nuovo>Oggetto).
   - **b.** Selezionare **hpqTarget** (Destinazione hpq) dall'elenco di classi e fare clic su **OK**.
   - **c.** Immettere un nome e un cognome appropriati nella finestra di dialogo **New hpqTarget** (Nuova destinazione hpq). In questo esempio, il nome host DNS di iLO 2, *rib-email-server*, sarà utilizzato come nome dell'oggetto di gestione di Lights-Out, e il cognome sarà *RiLOEII*. Fare clic su **OK**. Verrà visualizzata la pagina Select Object Subtype (Seleziona sottotipo oggetto).
   - **d.** Selezionare **Lights Out Management Device** (Dispositivo di gestione Lights-Out) e fare clic su **OK**.

e. Ripetere il processo per gli altri processori iLO 2 con nomi DNS "*rib-nntp-server*" e "*rib-file-server-users1*" in *hp devices* sotto *region1* e "*rib-file-server-users2*" e "*rib-app-server*" in *hp devices* sotto *region2*.

3. Utilizzando gli snap-in di ConsoleOne forniti da HP, creare oggetti ruolo HP nell'unità organizzativa *roles*.

   a. Fare clic con il pulsante destro del mouse sull'unità organizzativa *roles* nell'unità organizzativa *region2* e selezionare *New*>**Object** (Nuovo>Oggetto).

   b. Selezionare **hpqRole** (Ruolo hpq) dall'elenco di classi e fare clic su **OK**.

   c. Immettere un nome appropriato nella pagina **New hpqRole** (Nuovo ruolo hpq). In questo esempio, il ruolo conterrà utenti qualificati per l'amministrazione del server remoto e si chiamerà "*remoteAdmins*". Fare clic su **OK**. Verrà visualizzata la pagina Select Object Subtype (Seleziona sottotipo oggetto).

   d. Poiché questo ruolo gestirà i diritti per i dispositivi di gestione Lights-Out, selezionare **Lights Out Management Devices** (Dispositivi di gestione Lights-Out) dall'elenco e fare clic su **OK**.

   e. Ripetere il processo creando un ruolo per i monitor dei server remoti, denominato "*remoteMonitors*", in *roles* in *region1*, e un ruolo "*remoteAdmins*" e uno "*remoteMonitors*" in *roles* in *region2*.

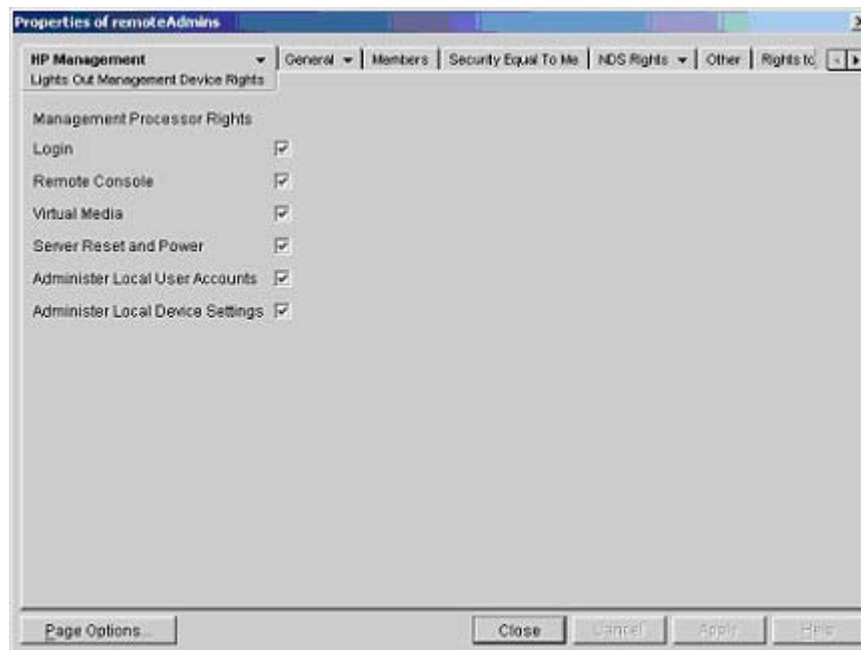
4. Utilizzando gli snap-in di ConsoleOne forniti da HP, assegnare diritti al ruolo e associare i ruoli a utenti e dispositivi.

   a. Fare clic con il pulsante destro del mouse su **remoteAdmins** nell'unità organizzativa *roles* dell'unità organizzativa *region1* e selezionare **Properties** (Proprietà).

   b. Selezionare la scheda **Role Managed Devices** (Dispositivi gestiti del ruolo) dell'opzione HP Management (Gestione HP) e fare clic su **Add** (Aggiungi).

   c. Utilizzando la pagina Select Objects (Seleziona oggetti), selezionare l'unità organizzativa *hp devices* nell'unità organizzativa *region1*. Selezionare i tre oggetti di gestione Lights-Out creati al passaggio 2. Fare clic su **OK**>**Apply** (OK>Applica).

d. Fare clic sulla scheda **Members** (Membri) e aggiungere utenti al ruolo facendo clic sul pulsante **Add** (Aggiungi) nella pagina Select Object (Seleziona oggetto). I dispositivi e gli utenti sono ora associati.

e. Utilizzare l'opzione Lights Out Management Device Rights (Diritti dei dispositivi di gestione Lights-Out) nella scheda HP Management (Gestione HP) per impostare i diritti per il ruolo. Tutti gli utenti di un ruolo avranno i diritti assegnati al ruolo su tutti i processori iLO 2 gestiti dal ruolo stesso. In questo esempio, gli utenti del ruolo *remoteAdmins* avranno accesso completo alle funzionalità di iLO 2. Selezionare le caselle accanto a ciascun diritto, quindi fare clic su **Apply** (Applica). Fare clic su **Close** (Chiudi) per chiudere il foglio delle proprietà.

5. Utilizzando la stessa procedura riportata al passaggio 4, modificare le proprietà del ruolo *remoteMonitors*:

a. Aggiungere i tre dispositivi iLO 2 in *hp devices* sotto *region1* all'elenco **Managed Devices** (Dispositivi gestiti) nell'area Role Managed Devices (Dispositivi gestiti del ruolo) della scheda HP Management (Gestione HP).

b. Aggiungere gli utenti al ruolo *remoteMonitors* tramite la scheda Members (Membri).

c. Selezionare la casella Login (Accesso) e fare clic su **Apply**>**Close** (Applica>Chiudi). Utilizzando l'opzione Lights Out Management Device Rights (Diritti dei dispositivi di gestione Lights-Out) nella scheda HP Management (Gestione HP), i membri del ruolo *remoteMonitors* potranno autenticare e visualizzare lo stato del server.

I diritti utente per ogni dispositivo LOM saranno la somma di tutti i diritti assegnati da tutti i ruoli in cui l'utente è membro e in cui il dispositivo LOM è un dispositivo gestito. Seguendo gli esempi precedenti, se un utente è presente nei ruoli *remoteAdmins* e *remoteMonitors* avrà tutti i diritti, poiché il ruolo *remoteAdmins* ha tali diritti.

Per configurare un dispositivo LOM e associarlo a un oggetto LOM utilizzato in questo esempio, le impostazioni devono essere simili a quelle della pagina Directory Settings (Impostazioni di directory) riportata di seguito.

NOTA: Per separare ciascun elemento nei nomi LDAP, si utilizza la virgola, non il punto.

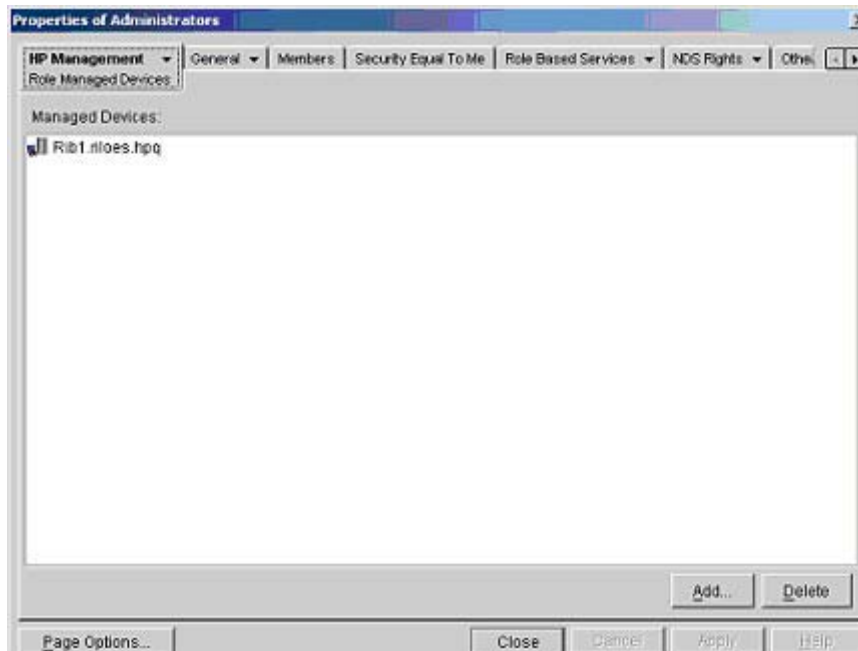
```
RIB Object DN = cn=rib-email-server,ou=hp devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

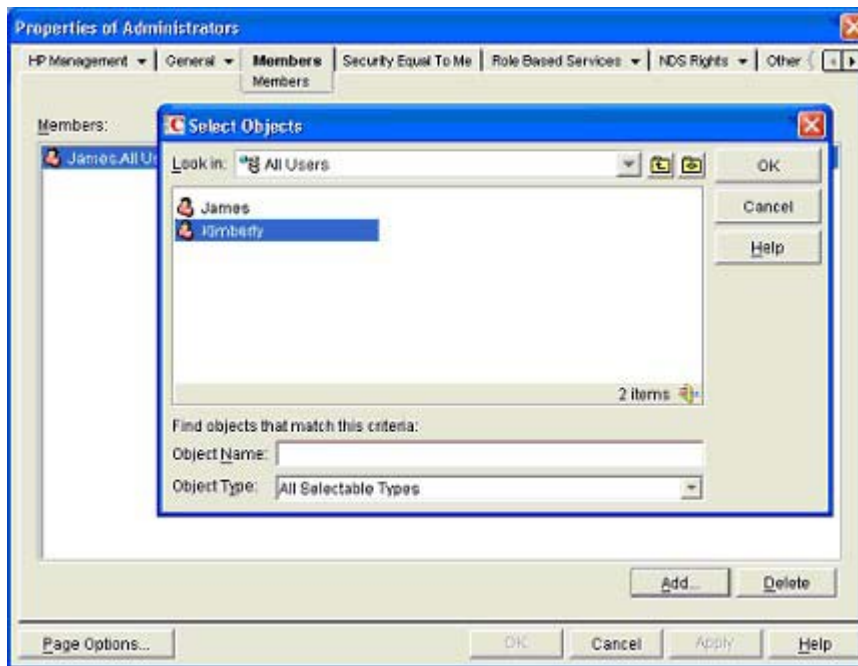
Se, ad esempio, l'utente *CSmith*, collocato nell'unità organizzativa *users* all'interno dell'azienda *samplecorp* e membro del ruolo *remoteAdmins* o *remoteMonitors*, desidera poter accedere a iLO 2, dovrà digitare `csmith` (distinzione tra maiuscole e minuscole) nel campo Login Name (Nome accesso) della schermata di accesso di iLO 2, quindi inserire la password di eDirectory nel campo Password disponibile nella stessa schermata.

Oggetti dei servizi di directory per eDirectory

Gli oggetti dei servizi di directory abilitano la virtualizzazione dei dispositivi gestiti e le relazioni tra il dispositivo gestito e l'utente o i gruppi già inclusi nel servizio di directory.

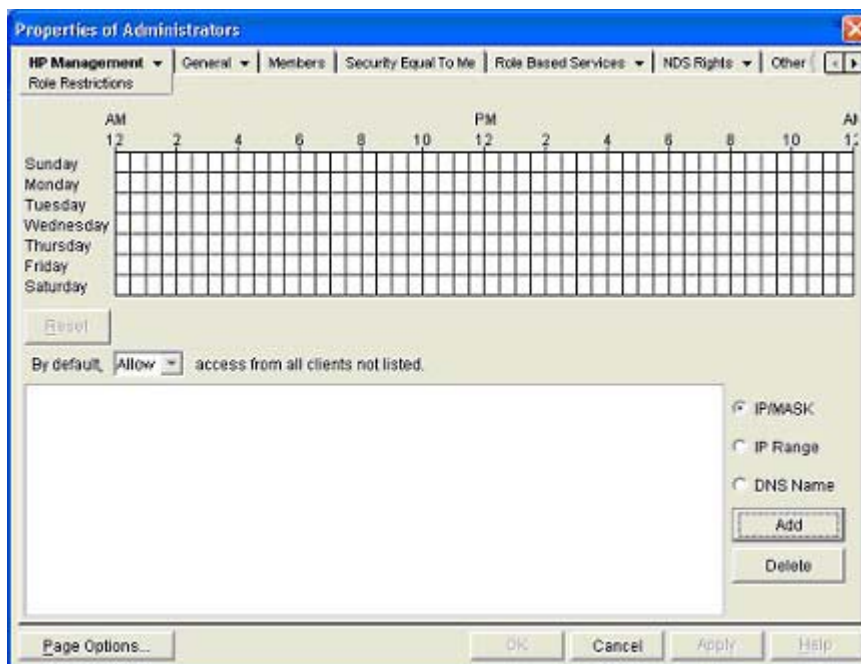
Dispositivi gestiti del ruolo

La sottoscheda Role Managed Devices (Dispositivi gestiti del ruolo) consente di aggiungere dispositivi HP da gestire all'interno di un ruolo. Facendo clic su **Add** (Aggiungi) è possibile selezionare il dispositivo HP specifico e aggiungerlo come dispositivo gestito.

Membri

Dopo aver creato gli oggetti utenti, la scheda Members (Membri) consentirà di gestire gli utenti all'interno del ruolo. Facendo clic su **Add** (Aggiungi), sarà possibile visualizzare l'utente specifico che si desidera aggiungere. Evidenziando un utente esistente e facendo clic su **Delete** (Elimina), l'utente verrà rimosso dall'elenco dei membri validi.

Restrizioni dei ruoli con eDirectory

La sottoscheda Role Restrictions (Restrizioni ruoli) consente di impostare le restrizioni di accesso per il ruolo. Queste restrizioni includono:

- Restrizioni temporali
- Restrizioni relative agli indirizzi IP di rete
  - IP/maschera
  - Intervallo IP

- Nome DNS

Restrizioni temporali

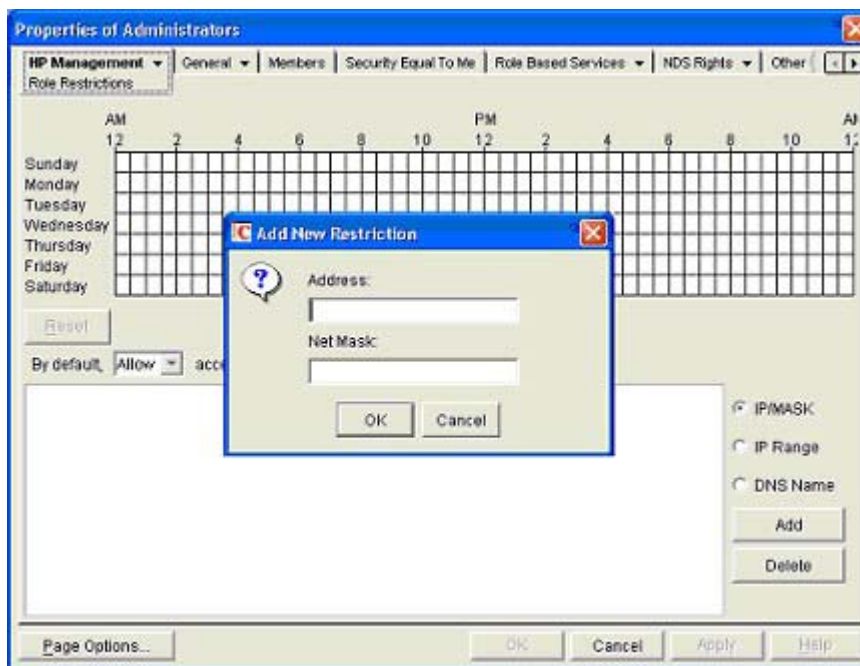
È possibile gestire le ore disponibili per l'accesso dei membri del ruolo utilizzando la griglia oraria visualizzata nella sottoscheda Role Restrictions (Restrizioni ruoli). È possibile selezionare le ore disponibili per l'accesso per ciascun giorno della settimana in incrementi 30 minuti. È possibile cambiare un singolo quadrato facendo clic su di esso oppure cambiare una sezione di quadrati facendo clic e tenendo premuto il pulsante del mouse, quindi trascinando il cursore sui quadrati da cambiare e rilasciando il pulsante del mouse. L'impostazione predefinita consente l'accesso in qualunque momento.

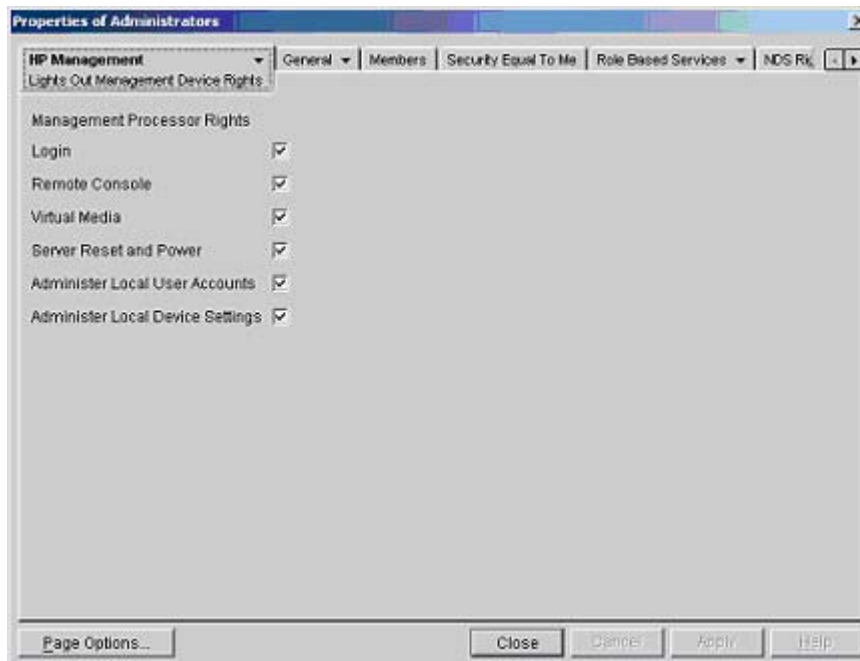
Indirizzo IP client forzato o accesso al nome DNS

È possibile concedere o negare l'accesso a un indirizzo IP, a un intervallo di indirizzi IP o ai nomi DNS.

1. Nel menu a discesa By Default (Impostazione predefinita) selezionare **Allow** (Permetti) o **Deny** (Nega) per concedere o negare l'accesso da tutti gli indirizzi, ad eccezione degli indirizzi IP, degli intervalli di indirizzi IP e dei nomi DNS specificati.
2. Selezionare gli indirizzi da aggiungere, selezionare il tipo di restrizione e fare clic su **Add** (Aggiungi).
3. Immettere le informazioni nella finestra a comparsa Add New Restriction (Aggiungi nuova restrizione) e fare clic su **OK**. Verrà visualizzata la finestra a comparsa Add New Restriction per l'opzione IP/Mask (IP/Maschera).

   L'opzione DNS Name (Nome DNS) consente di limitare l'accesso in base a un singolo nome DNS o a un sottodominio immesso nella forma host.azienda.com oppure *.dominio.azienda.com.
4. Fare clic su **Apply** (Applica) per salvare le modifiche.

Per rimuovere una o più voci, evidenziarle nell'elenco visualizzato e fare clic su **Delete** (Elimina).

Gestione Lights-Out di eDirectory

Dopo aver creato un ruolo, è possibile selezionare i diritti da assegnarvi. Gli utenti e gli oggetti dei gruppi possono divenire membri del ruolo per consentire l'assegnazione dei diritti associati a un singolo utente o a gruppi di utenti. I diritti vengono gestiti nella sottoscheda Lights Out Management Device Rights (Diritti dei dispositivi di gestione di Lights-Out) della scheda HP Management (Gestione HP).

Sono disponibili i seguenti diritti:

- Login (Accesso) – Questa opzione controlla se gli utenti possono collegarsi ai dispositivi associati.

  L'accesso Login permette di creare un utente con funzioni di service provider che riceve segnali di allarme da iLO 2 senza comunque avervi accesso.

- Remote Console (Console remota) – Questa opzione fornisce l'accesso dell'utente alla console remota.

- Virtual Media (Supporti virtuali) – Questa opzione permette l'accesso dell'utente alle funzionalità Virtual Floppy (Dischetto virtuale) e Virtual Media (Supporti virtuali) di iLO 2.

- Server Reset and Power (Reimpostazione e alimentazione server) – Questa opzione consente la reimpostazione o lo spegnimento remoto del server.

- Administer Local User Accounts (Amministra account utente locale) – Questa opzione permette l'amministrazione degli account. L'utente può modificare le impostazioni del proprio account, modificare le impostazioni degli account di altri utenti e aggiungere o eliminare altri utenti.

- Administer Local Device Settings (Amministra impostazioni dispositivo locale) – Questa opzione permette di configurare le impostazioni di iLO 2. Queste impostazioni includono le opzioni disponibili nelle schermate Global Settings (Impostazioni globali), Network Settings (Impostazioni di rete), SNMP Settings (Impostazioni SNMP) e Directory Settings (Impostazioni di directory) del browser di iLO 2.

Accesso utente mediante i servizi di directory

Nel campo Login Name (Nome accesso) della pagina di accesso di iLO 2 è possibile immettere:

- Gli utenti della directory

- I nomi distinti LDAP completi

  Esempio: CN=John Smith,CN=Utenti,DC=HP,DC=COM oppure @HP.com

  NOTA: La sola forma abbreviata del nome di accesso non indica alla directory il dominio al quale si sta tentando l'accesso. È infatti necessario fornire il nome utente o utilizzare il nome distinto LDAP dell'account corrente.

- Forma DOMINIO\nome utente (solo Active Directory)

  Esempio: HP\jsmith

- Forma nomeutente@dominio (solo Active Directory)

  Esempio: jsmith@hp.com

  NOTA: Gli utenti della directory specificati utilizzando la forma di ricerca @ possono trovarsi in uno dei tre contesti di ricerca configurati in Directory Settings (Impostazioni di directory).

- Forma nome utente

  Esempio: John Smith

  NOTA: Gli utenti della directory specificati utilizzando la forma nome utente possono trovarsi in uno dei tre contesti di ricerca configurati in Directory Settings (Impostazioni di directory).

- Utenti locali – Login-ID

  NOTA: Nella pagina di accesso di iLO 2, la lunghezza massima del nome di accesso è di 39 caratteri per gli utenti locali. Per gli utenti dei servizi di directory, la lunghezza massima del nome utente è di 256 caratteri.

6 Gestione remota abilitata alla directory

In questa sezione

Introduzione alla gestione remota abilitata alla directory

Questa sezione è rivolta agli amministratori che hanno già acquisito familiarità con i servizi di directory e con il prodotto iLO 2 e desiderano utilizzare la funzionalità di integrazione delle directory mediante lo schema HP per iLO 2. È necessario aver letto la sezione "Servizi di directory" (Servizi di directory a pagina 145) e aver acquisito le procedure di impostazione con i relativi esempi.

La gestione remota abilitata alla directory consente di:

- Creare oggetti di gestione Lights-Out

  Creare oggetti dispositivi LOM per la rappresentazione dei dispositivi che utilizzeranno i servizi di directory per l'autenticazione e l'autorizzazione degli utenti. Vedere la sezione "Servizi di directory" (Servizi di directory a pagina 145)" per ulteriori informazioni sulla creazione di oggetti di gestione Lights-Out per Active Directory (Servizi di directory per Active Directory a pagina 158) e eDirectory (Servizi di directory per eDirectory a pagina 169). Per creare gli oggetti, è possibile utilizzare gli snap-in forniti da HP. Si consiglia di assegnare nomi significativi agli oggetti dispositivo LOM, quali l'indirizzo di rete del dispositivo, il nome DNS, il nome del server host o il numero di serie.

- Configurare dispositivi di gestione Lights-Out

  Tutti i dispositivi LOM che utilizzano il servizio di directory per l'autenticazione e l'autorizzazione degli utenti devono essere configurati con le impostazioni di directory appropriate. Per informazioni dettagliate sulle impostazioni di directory specifiche, vedere "Configurazione delle impostazioni di directory (Configurazione delle impostazioni di directory a pagina 50)". Di norma, è possibile configurare ciascun dispositivo con l'indirizzo del server di directory appropriato, il nome distinto dell'oggetto LOM e gli eventuali contesti utente. L'indirizzo del server può essere costituito dall'indirizzo IP o dal nome DNS di un server di directory locale. Per una maggiore ridondanza, è possibile utilizzare un nome DNS multi-host.

Creazione di ruoli adeguati alla struttura organizzativa

Gli amministratori di un'organizzazione sono spesso posizionati in una struttura gerarchica nella quale gli amministratori subordinati devono assegnare diritti indipendentemente dal livello degli amministratori. In questo caso, è utile disporre di un ruolo che rappresenti i diritti assegnati dagli amministratori di livello superiore per consentire agli amministratori subordinati di creare e gestire i propri ruoli.

Uso di gruppi esistenti

Gli utenti e gli amministratori di molte aziende sono strutturati in gruppi. In molti casi, può risultare comodo utilizzare i gruppi esistenti e associarli a uno o più oggetti ruolo di gestione di Lights-Out. Quando i dispositivi sono associati agli oggetti ruoli, l'amministratore controlla l'accesso ai dispositivi Lights-Out associati al ruolo aggiungendo o eliminando membri dai gruppi.

Se si utilizza Microsoft® Active Directory, è possibile posizionare un gruppo all'interno di un altro gruppo o di gruppi nidificati. Gli oggetti ruolo sono considerati gruppi e possono contenere altri gruppi al loro interno. Aggiungere direttamente il gruppo nidificato esistente al ruolo e assegnare i diritti e le restrizioni appropriate. È possibile aggiungere nuovi utenti al gruppo esistente o al ruolo.

Novell eDirectory non consente l'uso di gruppi nidificati. Con eDirectory, gli utenti abilitati alla lettura di un ruolo sono considerati membri di tale ruolo. Quando si aggiunge un gruppo esistente, un'unità organizzativa o un'organizzazione a un ruolo, aggiungere l'oggetto come trustee di lettura del ruolo. Tutti i membri dell'oggetto sono considerati membri del ruolo. È possibile aggiungere nuovi utenti all'oggetto esistente o al ruolo.

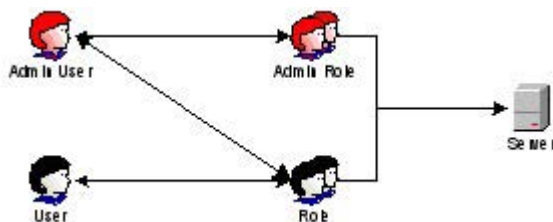
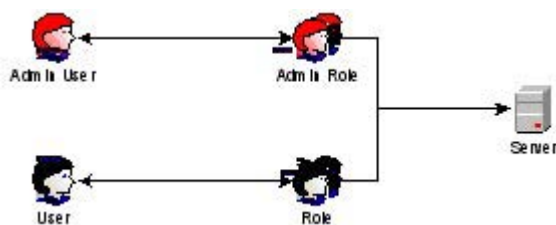
Se per estendere il gruppo del ruolo si utilizzano le assegnazioni dei diritti di directory o di trustee, è necessario che gli utenti siano in grado di leggere l'oggetto LOM che rappresenta il dispositivo LOM. Per l'autenticazione degli utenti, alcuni ambienti richiedono che lo stesso trustee del ruolo venga letto come trustee dell'oggetto LOM.

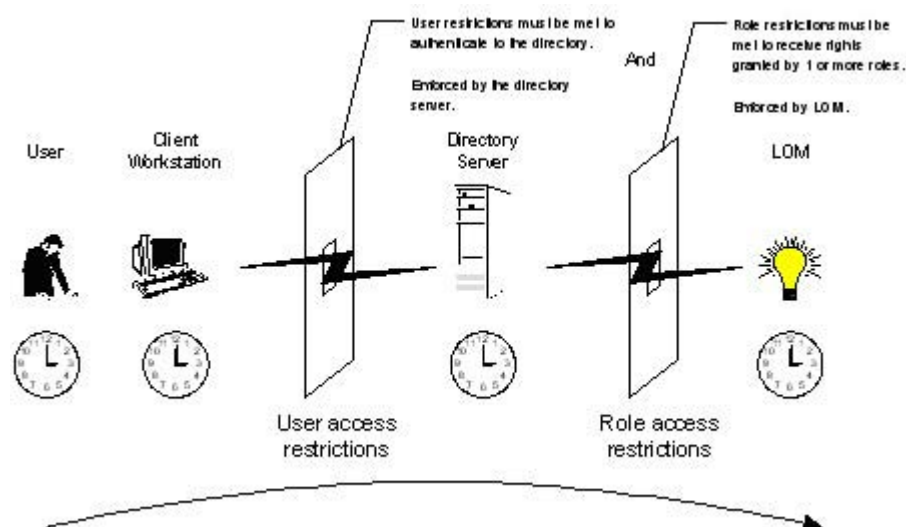
Uso di ruoli multipli

Nella maggior parte delle distribuzioni non è richiesto che il medesimo utente sia presente in più ruoli per la gestione dello stesso dispositivo. Tuttavia, questo tipo di configurazione è utile per la creazione di relazioni di diritti complesse. Nella creazione di relazioni di ruoli multipli, gli utenti ricevono tutti i diritti assegnati da ciascun ruolo applicabile. I ruoli possono solo concedere i diritti, mai revocarli. Se un ruolo concede un diritto a un utente, l'utente disporrà del diritto anche se si trova un altro ruolo che non concede tale diritto.

Di norma, un amministratore di directory crea un ruolo di base con un numero minimo di diritti assegnato e in seguito crea ruoli aggiuntivi per aggiungere diritti aggiuntivi. Questi ultimi vengono aggiunti in circostanze specifiche o a un sottoinsieme specifico di utenti del ruolo di base.

Ad esempio, un'organizzazione può avere due tipi di utenti, ovvero amministratori del dispositivo LOM o del server host e utenti del dispositivo LOM. In questa situazione, ha senso la creazione di due ruoli, uno per gli amministratori e uno per gli utenti. Entrambi i ruoli includono alcuni degli stessi dispositivi ma concedono diritti differenti. Talvolta, può essere utile assegnare diritti generici al ruolo inferiore e includere gli amministratori LOM nel ruolo oltre che nel ruolo amministrativo.

Un utente amministratore ottiene il diritto di accesso dal gruppo di utenti normale. Diritti superiori vengono assegnati dal ruolo di amministratore che assegna diritti aggiuntivi, quali la reimpostazione del server e la console remota.

Il ruolo di amministratore assegna tutti i diritti di amministrazione, quali la reimpostazione del server, la console remota e l'accesso.

Modalità di imposizione delle restrizioni di accesso alla directory

Due tipi di restrizioni limitano potenzialmente l'accesso di un utente della directory ai dispositivi LOM. Le restrizioni di accesso dell'utente ne limitano l'accesso all'autenticazione della directory. Le restrizioni di accesso del ruolo limitano la possibilità di un utente autenticato di ricevere i privilegi LOM basati sui diritti specificati in uno o più Ruoli.

Restrizione dei ruoli

Le restrizioni consentono agli amministratori di limitare l'ambito di un ruolo. Un ruolo concede i diritti solo agli utenti che soddisfano le restrizioni del ruolo. L'uso della restrizione dei ruoli consente di creare utenti con diritti dinamici che cambiano in base all'ora o all'indirizzo di rete del client.

NOTA: Quando le directory sono abilitate, l'accesso a un iLO 2 particolare dipende si basa sull'accesso in lettura dell'utente a un oggetto Role contenente il corrispondente oggetto iLO 2. Ciò include, in via esemplificativa, i membri elencati nell'oggetto Role. Se l'oggetto Role è impostato in modo da consentire la propagazione delle autorizzazioni ereditabili dall'oggetto principale, i membri di tale oggetto che dispongono dei privilegi di accesso in lettura avranno accesso anche a iLO 2. Per visualizzare l'elenco di controllo di accesso, passare a Utenti e computer, aprire la schermata delle proprietà dell'oggetto Role e selezionare la scheda **Sicurezza**.

Per istruzioni dettagliate sulla creazione di restrizioni di rete e temporali per un ruolo, vedere la sezione "Restrizioni dei ruoli di Active Directory" (Restrizioni dei ruoli di Active Directory a pagina 167) oppure "Restrizioni dei ruoli con eDirectory" (Restrizioni dei ruoli con eDirectory a pagina 175).

Restrizioni temporali dei ruoli

Gli amministratori possono impostare restrizioni temporali ai ruoli LOM. Agli utenti vengono concessi i diritti specifici per i dispositivi LOM elencati nel ruolo solo nel caso in cui gli utenti siano membri del ruolo e soddisfino le restrizioni temporali da esso previste.

I dispositivi LOM utilizzano l'ora locale dell'host per imporre le restrizioni temporali. Se l'orologio del dispositivo LOM non è impostato, l'applicazione della restrizione temporale del ruolo non riuscirà se non sono state specificate restrizioni temporali per il ruolo.

Le restrizioni temporali basate sul ruolo possono essere soddisfatte solo se è impostata l'ora sul dispositivo LOM. L'ora viene normalmente impostata all'avvio dell'host e viene conservata dagli agenti in esecuzione nel sistema operativo host che consente al dispositivo LOM di compensare gli anni bisestili e ridurre al minimo la deviazione dell'orologio rispetto all'host. Il verificarsi di eventi, quale una mancanza di corrente imprevista o la programmazione del firmware LOM, possono causare la reimpostazione dell'orologio del dispositivo LOM. Inoltre, per conservare l'ora nel corso delle programmazioni del firmware, è necessario che l'ora dell'host per il dispositivo LOM sia corretta.

Restrizioni dell'indirizzo del ruolo

Le restrizioni dell'indirizzo dei ruoli vengono imposte dal firmware LOM in base all'indirizzo di rete IP del client. Quando un ruolo soddisfa le restrizioni dell'indirizzo, vengono applicati i diritti concessi dal ruolo.

Le restrizioni dell'indirizzo possono risultare difficili da gestire in caso di tentativi di accesso tramite firewall o proxy di rete. Entrambi i sistemi possono modificare l'indirizzo di rete apparente del client, causando l'imposizione inaspettata delle restrizioni dell'indirizzo.

Restrizioni degli utenti

È possibile limitare gli accessi utilizzando restrizioni temporali e degli indirizzi.

Restrizioni dell'indirizzo utente

Gli amministratori possono assegnare restrizioni dell'indirizzo di rete all'account dell'utente della directory e tali restrizioni vengono imposte dal server di directory. Per i dettagli sull'imposizione delle restrizioni dell'indirizzo su client LDAP, quali l'accesso dell'utente a un dispositivo LOM, consultare la documentazione del servizio di directory.

Le restrizioni dell'indirizzo di rete assegnate all'utente della directory potrebbero non essere imposte nel modo previsto nel caso in cui l'utente della directory acceda tramite un server proxy. Quando un utente accede a un dispositivo LOM come utente della directory, il dispositivo LOM tenta l'autenticazione della directory utilizzando le restrizioni dell'indirizzo applicate a quell'utente. Tuttavia, poiché l'utente accede al dispositivo LOM attraverso un server proxy, l'indirizzo di rete del tentativo di autenticazione sarà quello del dispositivo LOM anziché quello della workstation client.

Restrizioni dell'intervallo degli indirizzi IP

Le restrizioni dell'intervallo di indirizzi IP consentono all'amministratore di specificare indirizzi di rete ai quali concedere o negare l'accesso. L'intervallo di indirizzi viene di norma specificato in un formato che inizia con l'indirizzo più basso e termina con l'indirizzo più alto. È possibile specificare un intervallo di indirizzi per concedere o negare l'accesso a un singolo indirizzo. Gli indirizzi che rientrano nell'intervallo di indirizzi IP specificato soddisfano la restrizione.

Restrizioni dell'indirizzo IP e della maschera di sottorete

Le restrizioni dell'indirizzo IP e della maschera di sottorete consentono all'amministratore di specificare un intervallo di indirizzi ai quali concedere o negare l'accesso. Questo formato offre funzioni simili all'intervallo di indirizzi IP ma potrebbe presentare caratteristiche più originali in base all'ambiente di

rete utilizzato. Un intervallo di indirizzi IP e maschere di sottorete viene di norma specificato utilizzando un maschera di bit dell'indirizzo di sottorete e dell'indirizzo che identifica gli indirizzi posti sulla stessa rete logica.

Secondo la logica binaria, se i bit dell'indirizzo di un computer client, al quale vengono aggiunti i bit della maschera di sottorete, corrispondono alla restrizione dell'indirizzo di sottorete, il computer client soddisfa la restrizione.

Restrizioni basate su DNS

Le restrizioni basate su DNS utilizzano il servizio di assegnazione dei nomi della rete per esaminare il nome logico del computer client, eseguendo la ricerca dei nomi di computer assegnati agli indirizzi IP del client. Le restrizioni DNS richiedono un server con nome funzionale. Se il servizio di assegnazione dei nomi si interrompe o non è raggiungibile, le restrizioni DNS non troveranno alcuna corrispondenza e non verranno eseguite.

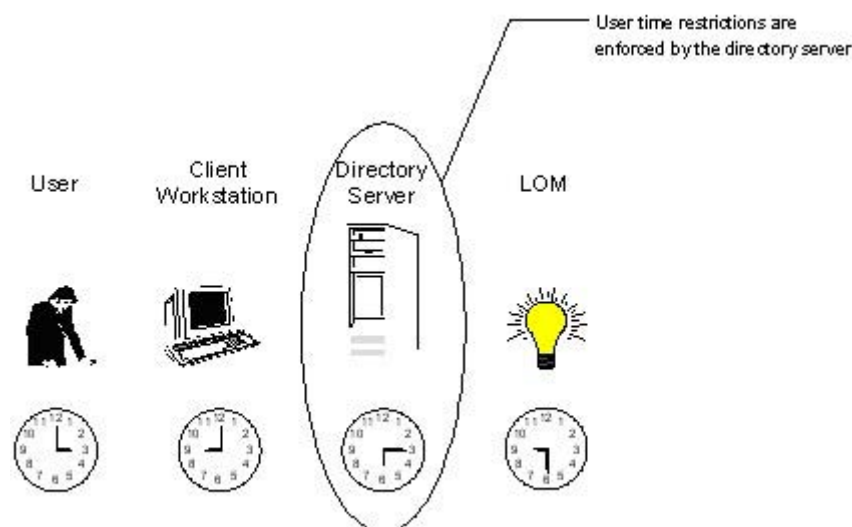
Le restrizioni basate su DNS possono limitare l'accesso a un nome di computer specifico o a computer che condividono un suffisso di dominio comune. Ad esempio, la restrizione DNS www.hp.com, troverà corrispondenza negli host ai quali è stato assegnato il nome di dominio www.hp.com. Tuttavia, la restrizione DNS *.hp.com troverà corrispondenza in tutti i computer di tipo HP.

Le restrizioni DNS possono generare ambiguità a causa della presenza di host multihomed (in esecuzione su più indirizzi IP). Le restrizioni DNS possono non trovare la perfetta corrispondenza con un singolo sistema.

L'uso delle restrizioni basate su DNS può causare alcuni problemi di protezione. I protocolli dei servizi nomi non sono sicuri. Eventuali utenti non autorizzati potrebbero accedere alla rete per inserire in rete un servizio DNS inaffidabile e creare falsi criteri di restrizione degli indirizzi. Per l'uso delle restrizioni degli indirizzi basate su DNS, è necessario implementare i criteri di protezione dell'organizzazione appropriati.

Modalità di imposizione delle restrizioni temporali dell'utente

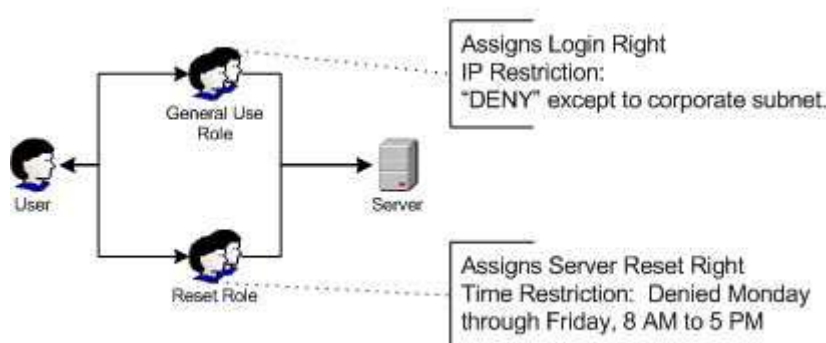
Gli amministratori possono assegnare una restrizione temporale agli account degli utenti della directory. Le restrizioni temporali limitano la possibilità dell'utente di accedere (eseguire l'autenticazione) alla directory. In genere, le restrizioni temporali vengono imposte utilizzando l'ora del server di directory. Nel caso in cui il fuso orario del server di directory sia diverso o l'accesso avvenga nei confronti di una replica in un differente fuso orario, sarà possibile utilizzare le informazioni relative al fuso orario dell'oggetto gestito per la regolazione dell'ora.

Il server di directory valuta le restrizioni temporali dell'utente. Tale processo può tuttavia risultare complicato a causa dei diversi fusi orari o del sistema di autenticazione.

Creazione di restrizioni e ruoli multipli

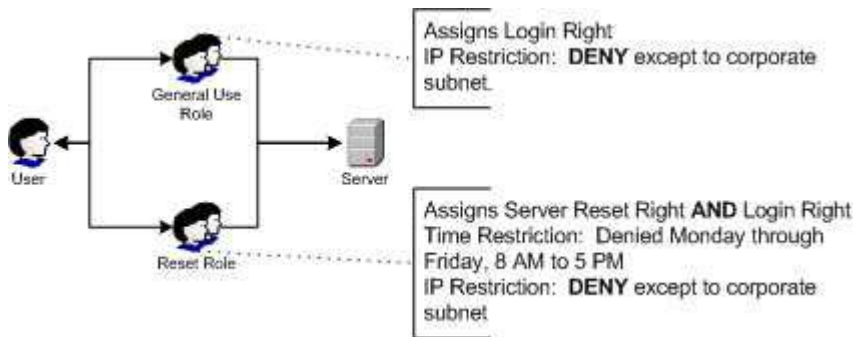
L'applicazione più utile dei ruoli multipli prevede la restrizione di uno o più ruoli per far sì che i diritti non vengano applicati in tutte le situazioni. Altri ruoli forniscono differenti diritti utilizzando restrizioni differenti. L'uso di restrizioni e ruoli multipli permette all'amministrazione la creazione arbitraria di relazioni di diritti complesse con un numero di ruoli minimo.

Ad esempio, un'organizzazione potrebbe disporre di un criterio di protezione che prevede la possibilità di uso del dispositivo LOM da parte degli amministratori LOM dall'interno della rete aziendale, ma che permetta loro la reimpostazione del server unicamente al di fuori del normale orario di lavoro.

Per gestire la situazione, gli amministratori di directory potrebbero essere tentati di creare due ruoli. In tal caso si consiglia la massima cautela. La creazione di un ruolo che fornisce i diritti di reimpostazione del server richiesti, limitandoli all'applicazione al di fuori dell'orario di lavoro, potrebbe consentire la reimpostazione del server agli amministratori esterni alla rete aziendale in contraddizione con la maggior parte dei criteri di protezione.

Nell'esempio fornito, il criterio di protezione prevede che l'uso generale sia limitato ai client inclusi nella sottorete aziendale e che la possibilità di reimpostare il server sia ulteriormente limitata al di fuori dell'orario di lavoro.

In alternativa, l'amministratore di directory potrebbe creare un ruolo che conceda il diritto di accesso limitandolo alla rete aziendale e creare quindi un altro ruolo che conceda solo i diritti di reimpostazione del server limitandone l'uso al di fuori dell'orario di lavoro. Si tratta di una configurazione più facile da

gestire ma più pericolosa, poiché nel tempo potrebbe essere creato un altro ruolo che garantisce il diritto di accesso agli utenti esterni alla rete aziendale, che potrebbe inavvertitamente concedere agli amministratori LOM, inclusi nel ruolo di reimpostazione del server, la possibilità di reimpostare il server anche dall'esterno della rete aziendale, posto che vengano soddisfatte le restrizioni temporali di quel ruolo.

La configurazione precedente soddisfa i criteri di protezione aziendale. Tuttavia, l'aggiunta di un altro ruolo che conceda i diritti di accesso può concedere inavvertitamente i privilegi di reimpostazione del server dall'esterno della rete aziendale oltre l'orario di lavoro. Una soluzione più gestibile consiste nell'assegnare restrizioni al ruolo di reimpostazione e al ruolo di uso generale.

Utilizzo degli strumenti di importazione principali

L'aggiunta e la configurazione di un gran numero di oggetti LOM richiede molto tempo. Per supportare lo svolgimento di queste attività, HP offre diverse utility.

- Utility di migrazione HP Lights-Out

  L'utility di migrazione HP Lights-Out (HPQLOMIG.EXE) consente di importare e configurare dispositivi LOM multipli. L'utility HPQLOMIG.EXE include un'interfaccia utente grafica che guida l'utente durante l'implementazione o l'aggiornamento di un gran numero di processori di gestione. HP consiglia di utilizzare l'interfaccia utente grafica durante l'aggiornamento di numerosi processori di gestione. Per ulteriori informazioni, vedere la sezione "Utility di migrazione delle directory HPQLOMIG" (Utility di migrazione delle directory HPQLOMIG a pagina 187).

- Utility di migrazione HP Lights-Out della riga di comando

  L'utility di migrazione HP Lights-Out della riga di comando (HPQLOMGC.EXE) permette di eseguire la migrazione tramite la riga di comando anziché l'interfaccia utente grafica. Questa utility viene utilizzata in combinazione con le funzionalità di Application Launch e di query di HP Systems Insight Manager e permette di configurare diversi dispositivi contemporaneamente. Per la configurazione di pochi dispositivi LOM, è preferibile utilizzare l'utility della riga di comando. Per ulteriori informazioni, vedere la sezione "Utility di migrazione delle directory HPQLOMIG" (Utility di migrazione delle directory HPQLOMIG a pagina 187).

- Utility HP SIM:

  - Gestire dispositivi LOM multipli.

  - Le applicazioni individuano i dispositivi LOM come processori di gestione utilizzando CPQLOCFG per l'invio di un file di script XML RIBCL a un gruppo di dispositivi LOM per la loro gestione. I dispositivi LOM eseguono quindi l'azione definita dal file RIBCL e inviano una risposta al file di registro di CPQLOCFG. Per ulteriori informazioni, consultare la *Guida delle risorse mediante la riga di comando e lo scripting del processore di gestione HP Integrated Lights-Out*.

- Utility di importazione tradizionali

Gli amministratori con conoscenza degli strumenti LDIFDE e NDS Import/Export Wizard possono utilizzare tali utility per importare o creare diversi oggetti LOM nella directory. Gli amministratori, tuttavia, devono configurare i dispositivi manualmente, come descritto in precedenza, anche se possono eseguire questa operazione in qualsiasi momento. Per creare gli oggetti dispositivo LOM con le stesse modalità utilizzate per la creazione degli utenti o di altri oggetti, è inoltre possibile utilizzare le interfacce programmatiche o di script. Nella sezione "Schema dei servizi di directory" (Schema dei servizi di directory a pagina 233) sono riportati i dettagli sugli attributi e i formati di dati degli attributi per la creazione degli oggetti di gestione Lights-Out.

7 Utility di migrazione delle directory HPQLOMIG

In questa sezione

Introduzione all'utility HPQLOMIG

L'utility HPQLOMIG è destinata ai clienti che dispongono di processori di gestione installati in precedenza e desiderano semplificare la migrazione di tali processori per la gestione in base a directory. HPQLOMIG consente di automatizzare alcuni dei passaggi di migrazione necessari per il supporto dei servizi di directory da parte dei processori di gestione. HPQLOMIG consente di effettuare le seguenti operazioni:

- Rilevare i processori di gestione sulla rete.
- Aggiornare il firmware dei processori di gestione alla versione in grado di supportare i servizi di directory o le directory senza schema.
- Assegnare un nome ai processori di gestione per la relativa identificazione nella directory.
- Creare oggetti nella directory corrispondenti a ciascun processore di gestione e associarli a un ruolo.
- Configurare i processori di gestione per abilitarli alla comunicazione con la directory.

Compatibilità

L'utility HPQLOMIG viene eseguita su Microsoft® Windows® e richiede l'installazione di Microsoft® .NET Framework. Per ottenere ulteriori informazioni su .NET Framework e scaricarne l'eseguibile, visitare il sito Web Microsoft® (http://www.microsoft.com/net). L'utility HPQLOMIG supporta i seguenti sistemi operativi:

- Active Directory
  - Windows® 2000
  - Windows® Server 2003
- Novell eDirectory 8.6.2
  - Windows® 2000
  - Windows® Server™ 2003

Pacchetto HP Lights-Out Directory

Tutto il software di migrazione, compresi gli snap-in di gestione e l'utility di estensione dello scherma, è incluso in un componente Smart HP. Per completare la migrazione dei processori di gestione, è necessario estendere lo schema e installare gli snap-in di gestione prima di eseguire lo strumento di migrazione. Per scaricare il componente Smart, visitare la sezione del sito Web HP relativa ai dispositivi di gestione Lights-Out (http://www.hp.com/servers/lights-out).

Per installare le utility di migrazione, fare clic su **LDAP Migration Utility** (Utility di migrazione LDAP) nel componente Smart. Viene avviato un programma di installazione MSI di Microsoft® che avvia e installa HPQLOMIG, le DLL necessarie, il contratto di licenza e altri file nella directory C:\Program Files \Hewlett-Packard\HP Lights-Out Migration Tool. È possibile selezionare una directory diversa. Il programma di installazione crea un collegamento a HPQLOMIG nel menu Start e installa un file XML di esempio.

NOTA: Se .NET Framework non è installato, l'utility di installazione visualizzerà un messaggio di errore e terminerà l'esecuzione.

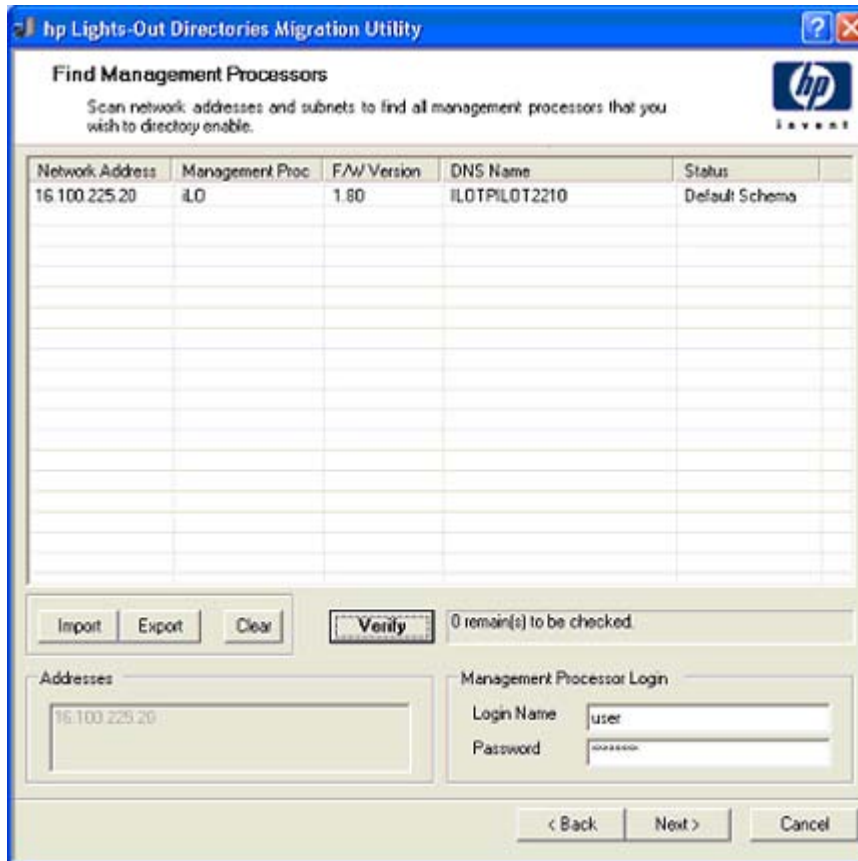
Utilizzo di HPQLOMIG

L'utility HPQLOMIG automatizza il processo di migrazione dei processori di gestione creando oggetti nella directory corrispondenti a ciascun processore di gestione e associandoli a un ruolo. L'utility HPQLOMIG dispone di un'interfaccia utente grafica e include procedure guidate per l'implementazione o l'aggiornamento di un gran numero di processori di gestione.

Individuazione dei processori di gestione

Il primo passaggio della migrazione consiste nel rilevamento di tutti i processori di gestione che si desidera abilitare ai servizi di directory. Per la ricerca dei processori di gestione, è possibile utilizzare i nomi DNS, gli indirizzi IP o i caratteri jolly dell'indirizzo IP. Per l'immissione delle variabili nel campo degli indirizzi, è necessario utilizzare le seguenti regole:

- I nomi DNS, gli indirizzi IP e i caratteri jolly degli indirizzi IP devo essere separati da un punto e virgola.
- Il carattere jolly dell'indirizzo IP è rappresentato dal carattere "*" nel terzo e quarto ottetto dei campi. Ad esempio, l'indirizzo IP 16.100.*.* è un indirizzo valido, mentre l'indirizzo IP 16.*.*.* non è un indirizzo valido.
- È anche possibile specificare gli intervalli utilizzando un trattino. Ad esempio, 192.168.0.2-10 è un intervallo valido. L'utilizzo del trattino è consentito solo nell'ottetto all'estrema destra.
- Dopo aver fatto clic su **Find** (Trova), l'utility HPQLOMIG avvia il ping e il collegamento alla porta 443 (porta SSL predefinita). Scopo di queste azioni è di determinare rapidamente se l'indirizzo di rete di destinazione è un processore di gestione. Se il dispositivo non risponde correttamente al ping o al collegamento alla porta 443, l'indirizzo rilevato non è un processore di gestione.

Se durante il rilevamento si seleziona **Next**, **Back** (Avanti, Indietro) o si chiude l'applicazione, le operazioni sull'indirizzo corrente vengono completate, mentre quelle sugli indirizzi di rete successivi vengono annullate.

Per avviare il processo di rilevamento dei processori di gestione, procedere come segue:

1. Fare clic su **Start** e selezionare **Programmi>Hewlett-Packard, HP Lights-Out Migration Utility** per avviare il processo di migrazione.
2. Fare clic su **Next** (Avanti) per oltrepassare la finestra di benvenuto.
3. Nel campo degli indirizzi, immettere le variabili per eseguire la ricerca dei processori di gestione.
4. Immettere il nome di accesso e la password, quindi fare clic su **Find** (Trova). Il pulsante Find (Trova) cambia in Verify (Verifica) una volta completata la ricerca.

   È inoltre possibile inserire un elenco di processori di gestione facendo clic su **Import** (Importa). Il file è un file di testo semplice con un solo processore di gestione per riga. I campi sono separati da punto e virgola e comprendono:

   ◦ Network Address (Indirizzo di rete)
   ◦ Management Processor Type (Tipo di processore di gestione)
   ◦ Firmware Version (Versione firmware)
   ◦ DNS Name (Nome DNS)
   ◦ User Name (Nome utente)
   ◦ Password
   ◦ Directory Configuration (Configurazione directory)

     Ad esempio, su una riga potrebbe essere riportato:

```
16.100.225.20;iLO;1.80;ILOTPILOT2210;user;password;Default Schema
```

Se per motivi di sicurezza nel file è preferibile non immettere nome utente e password, lasciare vuoti questi campi ma conservare i relativi punto e virgola.

Aggiornamento del firmware dei processori di gestione

La schermata Upgrade Firmware (Aggiorna firmware) consente di aggiornare i processori di gestione alla versione del firmware che supporta le directory. Questa schermata consente inoltre di indicare la posizione dell'immagine del firmware di ciascun processore di gestione digitandone il percorso o facendo clic su **Browse** (Sfoglia).

NOTA: È necessario che le immagini binarie del firmware dei processori di gestione siano accessibili dal sistema sul quale è in esecuzione l'utility di migrazione. È possibile scaricare le immagini binarie dal sito Web HP (http://www.hp.com/servers/lights-out).

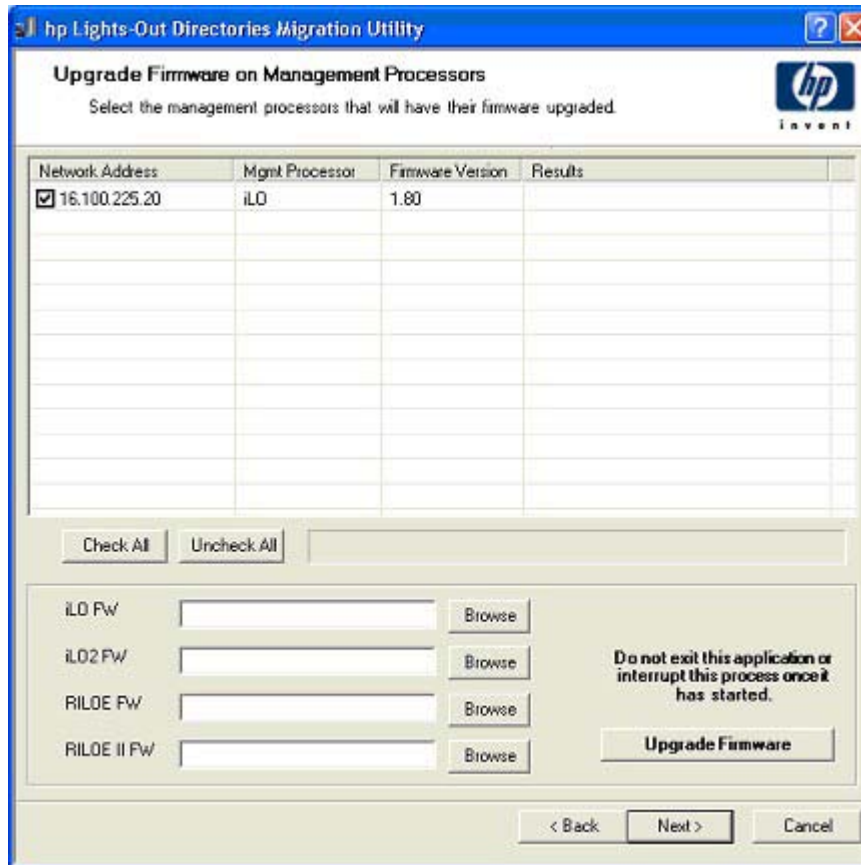
Processore di gestione	Versione minima del firmware
RILOE	2.50
RILOE II	1.10
iLO (Porta: iLO)	1.40
iLO 2	1.00

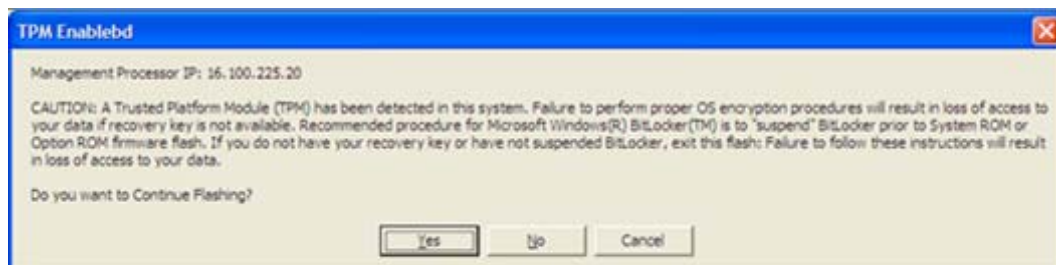
Il processo di aggiornamento potrebbe richiedere molto tempo, a seconda del numero di processori di gestione selezionati. Il completamento dell'aggiornamento del firmware di un singolo processore di gestione può richiedere fino a 5 minuti. Se l'aggiornamento non riesce, verrà visualizzato un messaggio nella colonna dei risultati e l'utility HPQLOMIG continuerà l'aggiornamento degli altri processori di gestione rilevati.

NOTA: Prima di eseguire l'utility su una rete di produzione, HP consiglia di verificare e il processo di aggiornamento e controllare i risultati in un ambiente di test. Il trasferimento incompleto dell'immagine del firmware al processore di gestione può richiedere la riprogrammazione locale del processore tramite un dischetto.

Per aggiornare il firmware dei processori di gestione, procedere come segue:

1. Selezionare il processore di gestione da aggiornare.
2. Per ciascun tipo di processore di gestione rilevato, immettere il percorso corretto per l'immagine del firmware oppure selezionare l'immagine.
3. Fare clic su **Upgrade Firmware** (Aggiorna firmware). I processori di gestione selezionati saranno aggiornati. Sebbene questa utility permetta di aggiornare centinaia di processori di gestione, è possibile aggiornare contemporaneamente solo 25 processori di gestione. L'attività di rete risulta piuttosto elevata durante questo processo.

4. Al termine dell'aggiornamento, fare clic su **Next** (Avanti).

Durante il processo di aggiornamento del firmware, tutti i pulsanti vengono disattivati per impedirne la selezione. Per chiudere l'applicazione, è anche possibile utilizzare la "X" posta nella parte superiore destra della schermata. Se l'interfaccia utente grafica viene chiusa durante la programmazione del firmware, l'applicazione continuerà ad essere eseguita in background e completerà l'aggiornamento del firmware su tutti i dispositivi selezionati.

HPLOMIG supporta l'aggiornamento flash del firmware sui server con un chip TPM. Se sul server è presente un modulo TPM abilitato e l'opzione Optional ROM measuring (Misurazione ROM opzionale) è abilitata, HPLOMIG visualizza un messaggio di avviso (mostrato di seguito). If you select Yes, HPLOMIG will continue with the flash process. Otherwise firmware flash on the selected server is skipped (Selezionando Yes (Sì), HPLOMIG continuerà con il processo flash. In caso contrario, l'aggiornamento flash del firmware sul server selezionato non verrà eseguito). Questo messaggio viene visualizzato ogni volta che, durante l'aggiornamento flash del firmware, viene rilevato un modulo TPM.

Selezione di un metodo di accesso alla directory

Dopo la pagina Firmware Upgrade (Aggiorna firmware), verrà visualizzata la pagina Select Directory Access Method (Seleziona metodo di accesso alla directory). È possibile selezionare i processori di gestione da configurare (rispetto all'uso dello schema) e la relativa modalità di configurazione. La pagina Select Directory Access Method (Seleziona metodo di accesso alla directory) consente di evitare la sovrascrittura accidentale dei processori iLO 2 già configurati per gli schemi HP o di quelli per i quali le directory sono state disattivate.

Questa pagina determina inoltre le pagine successive: schema HP Extended (HP esteso), senza schema (schema predefinito) o nessuna pagina di configurazione del supporto delle directory.

Per configurare il processore di gestione per:

- I servizi di directory, vedere la sezione "Configurazione delle directory quando è selezionato uno schema HP esteso" (Configurazione delle directory quando è selezionato uno schema HP esteso a pagina 194).
- Il supporto di directory senza schema (schema predefinito), vedere la sezione "Configurazione dell'integrazione di directory senza schema" (Configurazione dell'integrazione di directory senza schema a pagina 149).

Assegnazione dei nomi dei processori di gestione

Questa schermata consente di assegnare un nome agli oggetti dispositivo di gestione Lights-Out nella directory e creare oggetti dispositivo corrispondenti per tutti i processori di gestione che si desidera gestire. Per creare i nomi, è possibile:

- Utilizzare l'indirizzo di rete
- Utilizzare il nome DNS
- Utilizzare un indice
- Definire il nome manualmente
- Aggiungere un prefisso a tutti i nomi
- Aggiungere un suffisso a tutti i nomi

Per assegnare il nome ai processori di gestione, fare clic sul campo **Name** (Nome) e immettere il nome oppure:

1. Selezionare **Use Network Address** (Usa indirizzo di rete) **Use DNS Names** (Usa nomi DNS) o **Create Name Using Index** (Crea nome utilizzando un indice). È anche possibile denominare ciascun oggetto di directory del processore di gestione facendo clic due volte sul nome del campo con un lieve intervallo tra i clic.
2. Immettere il testo da aggiungere (suffisso o prefisso) a tutti i nomi (facoltativo).
3. Fare clic su **Generate Names** (Genera nomi). I nomi generati verranno visualizzati nella colonna Name (Nome). A questo punto, i nomi non sono stati scritti nella directory o nei processori di gestione, Vengono memorizzati fino alla pagina successiva.
4. (Facoltativo) Per modificare i nomi, fare clic su **Clear All Names** (Cancella tutti i nomi) e rinominare i processori di gestione.

5. Quando i nomi sono corretti, fare clic su **Next** (Avanti).

Configurazione delle directory quando è selezionato uno schema HP esteso

La schermata Configure Directory (Configura directory) consente di creare un oggetto dispositivo per ciascun processore di gestione rilevato e associare il nuovo oggetto dispositivo a un ruolo definito in precedenza. Ad esempio, la directory definisce un utente come membro di un ruolo (ad esempio, l'amministratore) dotato di una serie di privilegi per l'oggetto dispositivo specifico (ad esempio, una scheda RILOE II).

La schermata di configurazione della directory contiene i seguenti campi:

- **Network Address** (Indirizzo di rete) – Indica l'indirizzo di rete del server delle directory e può essere un nome DNS o un indirizzo IP valido.
- **Porta** (Porta) – La porta SSL per la directory. Il valore predefinito è 636. I processori di gestione possono comunicare con la directory solo attraverso la porta SSL.
- **Login Name** (Nome di accesso) e **Password** – Questi campi consentono di accedere a un account che dispone dei privilegi di accesso alla directory dell'amministratore di dominio.
- **Container DN** (Nome distinto contenitore) – Una volta impostati l'indirizzo di rete, la porta e le informazioni di accesso, è possibile fare clic su **Browse** (Sfoglia) per selezionare il contenitore e il nome distinto del ruolo. Il nome distinto del contenitore rappresenta la posizione in cui l'utility di migrazione creerà tutti gli oggetti dei processori di gestione nella directory.
- **Role DN** (Ruolo DN) – Nome distinto del ruolo che rappresenta la posizione in cui risiede il ruolo da associare agli oggetti dispositivo, da creare prima di eseguire l'utility.

Per configurare gli oggetti dispositivo da associare a un ruolo:

1. Immettere l'indirizzo di rete, il nome di accesso e la password per il server di directory richiesto.
2. Nel campo Container DN (Nome distinto contenitore), immettere il nome distinto del contenitore oppure fare clic su **Browse** (Sfoglia).
3. Fare clic su **Browse** (Sfoglia) oppure immettere il nome distinto del ruolo nel campo Role DN (Nome distinto ruolo) per associare gli oggetti dispositivo a un membro di un ruolo.
4. Fare clic su **Update Directory** (Aggiorna directory). Verrà eseguito il collegamento alla directory e saranno creati gli oggetti del processore di gestione che saranno quindi aggiunti ai ruoli selezionati.
5. Dopo avere associato gli oggetti dispositivo a un ruolo, fare clic su **Next** (Avanti).

Configurazione delle directory quando è selezionata l'integrazione senza schema

La schermata di configurazione dei processori di gestione contiene i seguenti campi:

- **Network Address** (Indirizzo di rete) – Indica l'indirizzo di rete del server delle directory e può essere un nome DNS o un indirizzo IP valido.
- **Login Name** (Nome di accesso) e **Password** – Questi campi consentono di accedere a un account che dispone dei privilegi di accesso alla directory dell'amministratore di dominio.
- **Security Group Distinguished Name** (Nome distinto del gruppo di protezione) – Il nome distinto del gruppo nella directory contenente un gruppo di utenti di iLO 2 con un insieme comune di

privilegi. Se il nome della directory, il nome di accesso e la password sono corretti, è possibile fare clic sul pulsante **Browse** (Sfoglia) per passare al gruppo e selezionarlo.

- **Privileges** (Privilegi) – I privilegi di iLO 2 associati al gruppo selezionato. Il privilegio di accesso è implicito se l'utente è un membro del gruppo.

Le impostazioni di configurazione dei processori di gestione sono memorizzate fino alla pagina successiva dell'installazione guidata.

Configurazione dei processori di gestione per le directory

L'ultimo passaggio del processo di migrazione è rappresentato dalla configurazione dei processori di gestione per la comunicazione con la directory. Questa schermata consente di creare dei contesti utente.

I contesti utente permettono di accedere utilizzando nomi oggetto utente o brevi anziché il nome distinto completo. Ad esempio, il contesto utente CN=Utenti,DC=RILOETEST2,DC=HP consente all'utente "John Smith" di accedere utilizzando John Smith anziché CN=John Smith,CN=Utenti, DC=RILOETEST2,DC=HP. È supportato anche il formato @. Ad esempio, la stringa @RILOETEST2.HP in un campo contesto consente all'utente di accedere utilizzando jsmith (supponendo che jsmith sia il nome utente breve).

Per configurare i processori di gestione per la comunicazione con la directory:

1. Immettere i contesti utente oppure scegliere **Browse** (Sfoglia).
2. Per le opzioni Directories Support (Supporto di directory) e Local Accounts (Account locali), selezionare **Enabled** (Abilitato) o **Disabled** (Disabilitato).

   Se il supporto di directory e gli account locali sono entrambi disabilitati, l'accesso remoto risulterà disabilitato. Per ripristinare l'accesso, riavviare il server ed eseguire l'utility F8 RBSU.

3. Fare clic su **Configure** (Configura). L'utility di migrazione si collegherà a tutti i processori di gestione selezionati e ne aggiornerà la configurazione secondo quanto specificato dall'utente. HPLOMIG supporta la configurazione di 15 contesti utente. Per accedere ai campi di contesti utente, utilizzare la barra di scorrimento.

Quando si fa clic su Configure (Configura), HPLOMIG visualizza il seguente messaggio:

Il messaggio indica che i 15 contesti utente sono applicabili solo a computer iLO 2 con una versione di firmware supportata (1.75 o successiva). Per tutti gli altri processori di gestione, sono applicabili solo i primi tre campi User Context (Contesto utente).

4. Al termine del processo, fare clic su **Done** (Chiudi).

8 Integrazione di HP Systems Insight Manager

In questa sezione

Integrazione di iLO 2 con HP SIM

Nei principali ambienti operativi, iLO 2 è completamente integrato con HP SIM. La completa integrazione con Systems Insight Manager offre inoltre una console di gestione singola per l'avvio di un browser Web standard da utilizzare per l'accesso. Tramite HP SIM è possibile stabilire una connessione a iLO 2 durante l'esecuzione del sistema operativo.

L'integrazione con HP SIM offre:

- Supporto per la consegna di trap SNMP a una console di HP SIM

  È possibile configurare la consegna alla console di HP SIM per l'inoltro di trap SNMP a un cercapersone o a un indirizzo di posta elettronica.

- Supporto per la gestione SNMP

  Grazie a iLO 2, HP SIM può accedere alle informazioni degli agenti Insight Management.

- Supporto per un processore di gestione

  HP SIM fornisce inoltre il supporto per un nuovo tipo di dispositivo, ovvero il processore di gestione. Tutti i dispositivi di iLO 2 installati sui server della rete vengono rilevati da HP SIM come processori di gestione. I processori di gestione sono associati ai server sui quali sono installati.

- Raggruppamento dei processori di gestione iLO 2

  Tutti i dispositivi iLO 2 possono essere raggruppati in modo logico e visualizzati su un'unica pagina. Questa funzionalità consente di accedere a iLO 2 da un solo punto di HP SIM.

- Collegamenti ipertestuali a iLO 2

  HP SIM fornisce un collegamento ipertestuale sulla pagina del server per l'avvio e il collegamento a iLO 2.

- HP Insight Agents

iLO 2, in combinazione con HP Management Agents, fornisce l'accesso remoto alle informazioni di gestione del sistema mediante l'interfaccia del browser Web di iLO 2.

Panoramica sul funzionamento di HP SIM

HP SIM consente di:

- Identificare i processori iLO 2.
- Creare un'associazione tra iLO 2 e il relativo server.
- Creare collegamenti tra iLO 2 e il relativo server.
- Visualizzare le informazioni e lo stato di iLO 2 e del server.
- Controllare la quantità di informazioni dettagliate visualizzate per iLO 2.
- Rappresentare visivamente l'infrastruttura del rack ProLiant BL p-Class.

Nelle seguenti sezioni viene brevemente descritta ognuna di queste funzioni. Per informazioni dettagliate sui vantaggi e sulle modalità di utilizzo di HP SIM, consultare la guida *HP Systems Insight Manager Technical Reference Guide* (Guida tecnica di riferimento per HP Systems Insight Manager) fornita con HP SIM e disponibile sul sito Web HP (http://www.hp.com/go/hpsim).

Impostazione della modalità SSO con HP SIM

1. Selezionare un iLO 2 ed effettuare l'accesso utilizzando le credenziali di amministratore.
2. Selezionare la scheda **Administration** (Amministrazione).
3. Nel menu visualizzato selezionare **Security** (Protezione).
4. Selezionare la scheda **HP SIM SSO**.
5. Impostare la modalità di attendibilità Single Sign-On su **Trust by Certificate** (Considera attendibile per certificato) e fare clic su **Apply** (Applica).
6. Fare clic su **Add HP SIM Server** (Aggiungi server HP SIM). Viene visualizzata la pagina HP Systems Insight Manager Single Sign-On Settings (Impostazioni Single Sign-On di HP Systems Insight Manager).
7. Nella pagina Retrieve and import a certificate from a trusted HP SIM Server (Recupera e importa certificato da server HP SIM attendibile), immettere il nome host o l'indirizzo IP del server HP SIM e fare clic su **Import Certificate** (Importa certificato). Il server viene aggiunto all'elenco dei server HP SIM attendibili nella scheda HP SIM SSO.
8. Accedere al server HP SIM aggiunto al passaggio 7 ed eseguire il rilevamento (discovery) di <LOM_server_name>. Al termine del processo di rilevamento, la modalità SSO è abilitata anche per questo iLO 2.

   Per ulteriori informazioni sulle attività di rilevamento, consultare la *HP Systems Insight Manager Technical Reference Guide* (Guida tecnica di riferimento per HP Systems Insight Manager). Per ulteriori informazioni sulle opzioni SSO di iLO 2, vedere la sezione "HP SIM SSO" (HP SIM SSO a pagina 56).

Identificazione e associazione di HP SIM

HP SIM è in grado di identificare un processore iLO 2 e creare un'associazione tra iLO 2 e il server. L'amministratore del dispositivo LOM può configurare iLO 2 affinché risponda alle richieste di identificazione di HP SIM.

Stato di HP SIM

In HP SIM, iLO 2 è identificato come processore di gestione. HP SIM visualizza lo stato del processore di gestione all'interno dell'elenco di sistema.

Il processore di gestione iLO 2 viene visualizzato sotto forma di icona nell'elenco dei dispositivi sulla stessa riga del server host corrispondente. Il colore dell'icona rappresenta lo stato del processore di gestione.

Per un elenco completo dei diversi stati del dispositivo, consultare la guida *HP Systems Insight Manager Technical Reference Guide* (Guida tecnica di riferimento per HP Systems Insight Manager) disponibile sul sito Web HP (http://www.hp.com/go/hpsim).

Collegamenti di HP SIM

Per facilitare la gestione, HP SIM crea collegamenti alle seguenti posizioni:

- iLO 2 e il server host di qualsiasi elenco di sistema
- Il server della pagina System Page (Pagina di sistema) di iLO 2
- iLO 2 della pagina System Page (Pagina di sistema) del server

Nelle pagine Systems List (Elenco di sistema) vengono visualizzati iLO 2, il server e la relazione tra iLO 2 e il server. Ad esempio, nella pagina possono essere visualizzati il server, il nome iLO 2 accanto al server e *nome iLO 2***IN***server* nel campo System Name (Nome sistema) per iLO 2.

Facendo clic sull'icona di stato di iLO 2, viene avviata la relativa interfaccia Web. Facendo clic sull'icona dello stato hardware, si avvia invece Insight Management Agents per il dispositivo. Facendo clic sul nome di iLO 2 o del server, viene visualizzata la pagina System Page (Pagina di sistema) del dispositivo.

La pagina System Page (Pagina di sistema) include le schede Identity (Identità), Tools & Links (Strumenti e Collegamenti) ed Event (Evento). Queste schede forniscono le informazioni sull'identità, lo stato, l'evento e i collegamenti per il dispositivo associato.

Elenchi di sistema di HP SIM

In HP SIM è possibile visualizzare i processori di gestione iLO 2. Gli utenti con diritti di configurazione completi possono creare e utilizzare insiemi di sistemi personalizzati per il raggruppamento dei processori di gestione. Per informazioni dettagliate, consultare la guida *HP Systems Insight Manager Technical Reference Guide* (Guida tecnica di riferimento per HP Systems Insight Manager) disponibile sul sito Web HP (http://www.hp.com/go/hpsim).

Ricezione di allarmi SNMP in HP SIM

È possibile configurare iLO 2 per l'inoltro di allarmi provenienti dagli agenti di gestione del sistema operativo host e per l'invio di allarmi generati da iLO 2 a HP SIM.

Systems Insight Manager fornisce il supporto per la gestione SNMP completa. iLO 2 supporta inoltre l'invio di trap SNMP a HP SIM. È possibile visualizzare il registro eventi, selezionare l'evento e visualizzare ulteriori informazioni sull'allarme.

La configurazione della ricezione degli allarmi SNMP in HP SIM è un processo a due fasi. Il processo richiede che HP SIM rilevi iLO 2 e lo configuri per l'abilitazione degli allarmi SNMP.

1. Per abilitare iLO 2 all'invio di trap SNMP, selezionare **SNMP/Insight Manager Settings** (Impostazioni SNMP/Insight Manager) nella scheda Administration (Amministrazione) del riquadro di spostamento di iLO 2. Viene abilitato l'invio di allarmi SNMP e viene fornito un indirizzo IP dei trap SNMP a iLO 2. Questo indirizzo IP deve coincidere con l'indirizzo del computer su cui è in esecuzione HP SIM. Vedere la sezione "Abilitazione degli allarmi SNMP" (Abilitazione degli allarmi SNMP a pagina 68).
2. Per rilevare iLO in HP SIM, configurare iLO 2 come un dispositivo gestito da HP SIM. L'aggiunta di iLO 2 a HP SIM consente al controller di rete su iLO 2 di funzionare come una porta di gestione dedicata, isolando il traffico di gestione dal controller di rete del server host remoto.
   - Avviare HP SIM.
   - Selezionare **Options>Discovery>Automatic Discovery** (Opzioni>Rilevamento>Rilevamento automatico).
   - Selezionare l'attività di rilevamento da eseguire e fare clic su Edit (Modifica).
   - Selezionare **IP range pinging** (Ping intervallo IP). Se l'indirizzo IP non è compreso nella sezione Ping inclusion ranges, templates, or hosts files (Intervalli inclusione ping, modelli o file host), immettere l'indirizzo IP.

- Fare clic su **OK**.
- Per aggiungere iLO 2 a HP SIM, effettuare una delle seguenti operazioni:
  - Fare clic su **Save and Run** (Salva e esegui). Al termine del processo di rilevamento, le query aggiuntive visualizzeranno il dispositivo come processore di gestione.

    Potrebbe essere necessario modificare la stringa di comunità di lettura SNMP, impostandola ad esempio su "public", in modo che iLO 2 venga visualizzato nell'elenco dei sistemi monitorati. Per modificare la stringa di comunità di lettura SNMP è possibile accedere alla pagina delle impostazioni dei protocolli di sistema selezionando **Options>Protocol Settings>System Protocol Settings** (Opzioni>Impostazioni protocollo>Impostazioni protocollo di sistema)
  - Fare clic su **Options>Protocol Settings>Global Protocol Settings** (Opzioni>Impostazioni protocollo>Impostazioni protocollo globali) e impostare le stringhe di comunità da utilizzare durante la rilevazione nella sezione Default SNMP Settings (Impostazioni SNMP predefinite). Al termine dell'impostazione, ripetere i passaggi a, b, c, d, e per eseguire il processo di rilevazione.

    Per i principali eventi non risolti, i trap di iLO 2 vengono visualizzati nella sezione All Events (Tutti gli eventi). Per ulteriori informazioni sull'evento, fare clic su **Event Type** (Tipo evento).

  NOTA: Per abilitare la gestione di iLO 2, è necessario installare gli agenti HP Insight per iLO 2 sul server host remoto. Per ulteriori informazioni sull'installazione e la configurazione degli agenti, vedere la sezione "Installazione dei driver di iLO 2".

Corrispondenza delle porte di HP SIM

HP SIM è configurato per l'avvio di una sessione HTTP per il controllo di iLO 2 sulla porta 80. È possibile cambiare il numero di porta. Se si desidera modificare il numero di porta, sarà necessario modificarlo anche in Network Settings (Impostazioni di rete) e HP SIM.

Per modificare il numero di porta in HP SIM, aggiungere la porta nel file config\identification \additionalWsDisc.props nella directory di installazione di HP SIM. La voce deve iniziare con il numero della porta HTTP per iLO 2. Se il numero di porta non viene modificato, non è necessario inserire alcuna voce in questo file per iLO 2. È importante che la voce sia costituita da un'unica riga e che inizi con il numero della porta, a cui devono seguire tutti gli elementi riportati nel seguente esempio.

L'esempio seguente mostra la voce da utilizzare per la rilevazione di iLO 2 sulla porta 55000 (immettere tutte le voci su una sola riga):

```
55000=iLO
2, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorPa
rser
```

Revisione delle informazioni sulla licenza per Advanced Pack in HP SIM

HP SIM visualizza lo stato della licenza dei processori di gestione iLO 2. È possibile utilizzare queste informazioni per determinare quanti e quali dispositivi iLO 2 dispongono di una licenza per iLO Advanced Pack.

Per visualizzare le informazioni sulla licenza, fare clic su **Deploy>License Manager>Manage Keys** (Distribuisci>Gestione licenze>Gestisci chiavi). Per assicurarsi che i dati siano aggiornati, eseguire

l'attività di identificazione dei sistemi per i processori di gestione. Per ulteriori informazioni sull'avvio delle attività, consultare la documentazione fornita con HP SIM.

9 Risoluzione dei problemi relativi a iLO 2

In questa sezione

Indicatori LED POST di iLO 2

Durante l'avvio iniziale di iLO 2, gli indicatori LED POST lampeggiano per segnalare l'avanzamento del processo di avvio di iLO 2, al termine del quale il LED HB (heartbeat, impulso vitale) lampeggia ogni secondo. Durante il normale funzionamento lampeggia in modo intermittente anche il LED 7.

Gli altri indicatori LED (da 1 a 6) si accendono dopo l'avvio del sistema per segnalare un problema di natura hardware. Se viene rilevato un errore hardware, reimpostare iLO 2. Per informazioni sulla posizione degli indicatori LED, consultare la documentazione del server.

Un errore di runtime di iLO 2 è segnalato dal continuo stato accesso o spento dei LED HB e LED 7. Lo stesso tipo di errore può essere segnalato anche dal continuo lampeggiamento dei LED. Se si verifica un errore di runtime, reimpostare iLO.

La sequenza dei LED 1, 2, 3, 4, 5, 6, 7 e 8 che lampeggiano in modo continuo, indica che iLO 2 non è stato aggiornato (aggiornamento firmware) e che si trova nella modalità di recupero dell'aggiornamento. Per ulteriori informazioni, vedere la sezione "Recupero dell'aggiornamento della rete iLO 2".

Gli indicatori LED sono assegnati nel modo seguente:

HB	7	6	5	4	3	2	1

Indicatore LED	Codice POST (attività completata)	Descrizione	Errore indicato
Nessuno	00	Selezione di chip di impostazione.	
1 o 2	02 – Funzionamento normale	Individuazione della piattaforma.	
2 e 1	03	Impostazione del bit RUNMAP.	
3	04	Inizializzazione del controller SDRAM.	
3 e 2	06	Attivazione della cache I.	
3, 2 e 1	07	Solo inizializzazione della cache D.	
4	08	Copia del dispositivo di caricamento secondario nella RAM.	Impossibile copiare il dispositivo di caricamento secondario.
4 e 1	09	Verifica del dispositivo di caricamento secondario.	Impossibile eseguire il dispositivo di caricamento secondario.
4 e 2	0a	Avvio del dispositivo di caricamento secondario.	Test della memoria SDRAM non riuscito.
4, 2 e 1	0b	Copia della ROM nella RAM.	Impossibile copiare il blocco di avvio.
4 e 3	0c	Verifica dell'immagine ROM nella RAM.	Impossibile eseguire il blocco di avvio.
4, 3 e 1	0d	Avvio blocco di avvio principale.	Il blocco di avvio non ha trovato un'immagine valida.
Nessuno		Avvio dell'inizializzazione di runtime C.	
4, 3 e 2	0e	Ricezione del controllo in Main().	Test automatico principale non riuscito.
Variabile	Variabile	Test automatico consentito per ogni sottosistema.	
4, 3, 2 e 1	0f	Avvio di ThreadX.	Avvio RTOS non riuscito.
Nessuno	00	Completamento di Main_init().	Avvio del sottosistema non riuscito.
HB e 7		Lampeggia quando il processore iLO 2 esegue il codice del firmware. Il valore dei sei indicatori LED più bassi non viene modificato.	

Il firmware del microprocessore di iLO 2 include il codice per l'esecuzione dei controlli di congruenza. Se uno di questi controlli non viene superato, il microprocessore esegue FEH (Fatal Exception Handler), che visualizza le informazioni mediante gli indicatori LED POST di iLO 2. I codici FEH si distinguono per il lampeggiamento alternato del numero 99 e la parte rimanente del codice di errore.

Codice FEH	Controllo di congruenza	Descrizione
9902	TXAPICHK	Una funzione RTOS è stata chiamata con un valore inappropriato o ha un'origine non corretta.
9903	TXCONTEXT	Il contesto salvato di uno o più thread è stato danneggiato.
9905	TRAP	Il test di uno stack non è riuscito, l'indirizzo restituito non è valido oppure è stata rilevata un'istruzione trap non ammessa.
9966	NMIWR	È stata eseguita una scrittura non prevista su una memoria insufficiente.
99C1	CHKNULL	Il vettore di reimpostazione è stato modificato.

Voci del registro eventi

Voce del registro eventi	Descrizione del registro eventi
Server power failed (Guasto di alimentazione al server)	Visualizza la data e l'ora in cui si è verificato il guasto di alimentazione del server.
Browser login (Accesso tramite browser): *Indirizzo IP*	Visualizza l'indirizzo IP del browser collegato.
Server power restored (Ripristino alimentazione al server)	Visualizza la data e l'ora in cui l'alimentazione al server è stata ripristinata.
Browser logout (Scollegamento del browser): *Indirizzo IP*	Visualizza l'indirizzo IP del browser scollegato.
Server reset (Reimpostazione del server)	Visualizza la data e l'ora di reimpostazione del server.
Failed Browser login – IP Address (Accesso tramite browser non riuscito – Indirizzo IP): *Indirizzo IP*	Visualizza la data e l'ora di un accesso non riuscito tramite browser.
iLO 2 Self Test Error (Errore del test automatico di iLO 2): #	Visualizza la data e l'ora in cui il test interno di iLO 2 non è riuscito. La causa è probabilmente il guasto di un componente critico. Si consiglia di non continuare ad utilizzare iLO 2 su questo server.
iLO 2 reset (Reimpostazione di iLO 2)	Visualizza la data e l'ora in cui iLO 2 è stato reimpostato.
On-board clock set; was #:#:#:#:#:# (Impostazione orologio incorporato: #:#:#:#:#:#)	Visualizza la data e l'ora in cui è stato impostato l'orologio incorporato.
Server logged critical error(s) (Errori critici registrati dal server)	Visualizza la data e l'ora in cui il server ha registrato degli errori critici.
Event log cleared by (Registro eventi cancellato da): *Utente*	Visualizza la data e l'ora in cui un utente ha cancellato il registro eventi.
iLO 2 reset to factory defaults (Reimpostazione di iLO 2 alle impostazioni predefinite in fabbrica)	Visualizza la data e l'ora in cui sono state ripristinate le impostazioni predefinite di iLO 2.
iLO 2 ROM upgrade to # (Aggiornamento della ROM iLO 2 il #)	Visualizza la data e l'ora in cui la ROM è stata aggiornata.
iLO 2 reset for ROM upgrade (Reimpostazione di iLO 2 per l'aggiornamento della ROM)	Visualizza la data e l'ora in cui iLO 2 viene reimpostato per l'aggiornamento della ROM.

Voce del registro eventi	Descrizione del registro eventi
iLO 2 reset by user diagnostics (Reimpostazione di iLO 2 mediante diagnostica utente)	Visualizza la data e l'ora in cui iLO 2 viene reimpostato mediante la diagnostica utente.
Power restored to iLO 2 (Reimpostazione alimentazione in iLO 2)	Visualizza la data e l'ora della reimpostazione dell'alimentazione in iLO 2.
iLO 2 reset by watchdog (Reimpostazione di iLO 2 mediante watchdog)	Visualizza la data e l'ora in cui iLO 2 è stato reimpostato a seguito di un errore. Se il problema persiste, contattare l'assistenza clienti.
iLO 2 reset by host (Reimpostazione di iLO 2 mediante host)	Visualizza la data e l'ora in cui il server reimposta iLO 2.
Recoverable iLO 2 error, code # (Errore reversibile di iLO 2, codice #)	Visualizza la data e l'ora in cui iLO 2 è stato reimpostato a seguito di un errore non critico. Se il problema persiste, contattare l'assistenza clienti.
SNMP trap delivery failure (Errore di invio trap SNMP): *Indirizzo IP*	Visualizza la data e l'ora in cui il trap SNMP non si è collegato all'indirizzo IP specificato.
Test SNMP trap alert failed for (Allarme trap SNMP di test non riuscito per): *Indirizzo IP*	Visualizza la data e l'ora in cui il trap SNMP non si è collegato all'indirizzo IP specificato.
Power outage SNMP trap alert failed for (Allarme trap SNMP di interruzione dell'alimentazione non riuscito per): *Indirizzo IP*	Visualizza la data e l'ora in cui il trap SNMP non si è collegato all'indirizzo IP specificato.
Server reset SNMP trap alert failed for (Allarme trap SNMP di reimpostazione del server non riuscito per): *Indirizzo IP*	Visualizza la data e l'ora in cui il trap SNMP non si è collegato all'indirizzo IP specificato.
Illegal login SNMP trap alert failed for (Allarme trap SNMP di accesso non valido non riuscito per): *Indirizzo IP*	Visualizza la data e l'ora in cui il trap SNMP non si è collegato all'indirizzo IP specificato.
Diagnostic error SNMP trap alert failed for (Allarme trap SNMP di errore diagnostica non riuscito per): *Indirizzo IP*	Visualizza la data e l'ora in cui il trap SNMP non si è collegato all'indirizzo IP specificato.
Host generated SNMP trap alert failed for (Allarme trap SNMP generato dall'host non riuscito per): *Indirizzo IP*	Visualizza la data e l'ora in cui il trap SNMP non si è collegato all'indirizzo IP specificato.
Network resource shortage SNMP trap alert failed for (Allarme trap SNMP di risorse di rete insufficienti non riuscito per): *Indirizzo IP*	Visualizza la data e l'ora in cui il trap SNMP non si è collegato all'indirizzo IP specificato.
iLO 2 network link up (Connessione di rete a iLO 2)	Visualizza la data e l'ora in cui è stata effettuata la connessione di rete a iLO 2.
iLO 2 network link up (Disconnessione di rete a iLO 2)	Visualizza la data e l'ora in cui iLO 2 non è collegato in rete.
iLO 2 Firmware upgrade started by (Aggiornamento del firmware di iLO 2 avviato da): *Utente*	Visualizza la data e l'ora in cui un utente ha avviato un aggiornamento del firmware.
Host server reset by (Server host reimpostato da): *Utente*	Visualizza la data e l'ora in cui un utente ha reimpostato il server host.
Host server powered OFF by (Server host spento da): *Utente*	Visualizza la data e l'ora in cui un utente ha spento un server host.
Host server powered ON by (Server host acceso da): *Utente*	Visualizza la data e l'ora in cui un utente ha acceso un server host.
Virtual Floppy in use by (Unità dischetto virtuale utilizzata da): *Utente*	Visualizza la data e l'ora in cui un utente ha iniziato ad utilizzare un'unità dischetto virtuale.
Remote Console login (Accesso da console remota): *Utente*	Visualizza la data e l'ora in cui un utente ha effettuato l'accesso a una sessione della console remota.
Remote Console Closed (Console remota chiusa)	Visualizza la data e l'ora in cui è stata chiusa una sessione della console remota.

Voce del registro eventi	Descrizione del registro eventi
Failed Console login - IP Address (Accesso console non riuscito - Indirizzo IP): *Indirizzo IP*	Visualizza un accesso console non riuscito con il relativo indirizzo IP.
Added User (Utente aggiunto): *Utente*	Visualizza la data e l'ora in cui è stato aggiunto un utente locale.
User Deleted by (Utente eliminato da): *Utente*	Visualizza la data e l'ora in cui è stato eliminato un utente locale.
Modified User (Utente modificato): *Utente*	Visualizza la data e l'ora in cui è stato modificato un utente locale.
Browser login (Accesso tramite browser): *Utente*	Visualizza la data e l'ora in cui un utente autorizzato ha effettuato l'accesso a iLO 2 tramite un browser Internet.
Browser logout (Scollegamento del browser): Utente	Visualizza la data e l'ora in cui un utente autorizzato si è scollegato da iLO 2 tramite un browser Internet.
Failed Browser login – IP Address (Accesso tramite browser non riuscito – Indirizzo IP): *Indirizzo IP*	Visualizza la data e l'ora di un accesso tramite browser non riuscito.
Remote Console login (Accesso da console remota): *Utente*	Visualizza la data e l'ora in cui un utente autorizzato ha effettuato l'accesso tramite la porta della console remota.
Remote Console Closed (Console remota chiusa)	Visualizza la data e l'ora in cui un utente autorizzato della console remota si è scollegato o la porta della console remota è stata chiusa in seguito a un tentativo di accesso non riuscito.
Failed Console login – IP Address (Accesso da console non riuscito - Indirizzo IP): *Indirizzo IP*	Visualizza la data e l'ora in cui un utente autorizzato ha eseguito tre tentativi di accesso non riusciti tramite la porta della console remota.
Added User (Utente aggiunto): *Utente*	Visualizza la data e l'ora in cui è stata inserita una nuova voce nell'elenco degli utenti autorizzati.
User Deleted by (Utente eliminato da): *Utente*	Visualizza la data e l'ora in cui una voce è stata rimossa dall'elenco degli utenti autorizzati. La sezione Utente visualizza l'utente che ha richiesto la rimozione.
Event Log Cleared (Cancellazione registro eventi): *Utente*	Visualizza la data e l'ora in cui l'utente ha cancellato il registro eventi.
Power Cycle (Reset) (Spegnimento/Accensione – Reimpostazione): *Utente*	Visualizza la data e l'ora della reimpostazione.
Virtual Power Event (Evento accensione virtuale): *Utente*	Visualizza la data e l'ora in cui è stato utilizzato il pulsante di accensione virtuale.
Security Override Switch Setting is On (Interruttore di esclusione della protezione attivato)	Visualizza la data e l'ora in cui il sistema viene avviato con l'interruttore di esclusione della protezione attivato.
Security Override Switch Setting Changed to Off (Interruttore di esclusione della protezione disattivato)	Visualizza la data e l'ora in cui il sistema viene avviato con l'interruttore di esclusione della protezione disattivato.
On-board clock set; was previously "[NOT SET]" (Orologio incorporato; impostato in precedenza su "[NOT SET]")	Visualizza la data e l'ora in cui è stato impostato l'orologio incorporato. Se in precedenza non è stata effettuata alcuna impostazione, viene visualizzata l'ora precedente o l'indicazione "NOT SET".
Logs full SNMP trap alert failed for (Allarme trap SNMP di registro pieno non riuscito per): *Indirizzo IP*	Visualizza il momento in cui i registri sono pieni e l'allarme trap SNMP non è riuscito per un indirizzo IP specificato.
Security disabled SNMP trap alert failed for (Protezione disabilitata e allarme trap SNMP non riuscito per): *Indirizzo IP*	Visualizza il momento in cui la protezione è stata disattivata e l'allarme trap SNMP non è riuscito per un indirizzo IP specificato.

Voce del registro eventi	Descrizione del registro eventi
Security enabled SNMP trap alert failed for (Protezione abilitata e allarme trap SNMP non riuscito per): *Indirizzo IP*	Visualizza il momento in cui la protezione è stata abilitata e l'allarme trap SNMP non è riuscito per un indirizzo IP specificato.
Virtual Floppy connected by (Unità dischetto virtuale connessa da) *utente*).	Visualizza la data e l'ora in cui un utente autorizzato ha effettuato il collegamento a un'unità dischetto virtuale.
Virtual Floppy connected by (Unità dischetto virtuale scollegata da) *utente*.	Visualizza la data e l'ora in cui un utente autorizzato si è scollegato da un'unità dischetto virtuale.
License added by (Licenza aggiunta da): *Utente*	Visualizza la data e l'ora in cui un utente autorizzato aggiunge una licenza.
License removed by (Licenza rimossa da): *Utente*	Visualizza la data e l'ora in cui un utente autorizzato rimuove una licenza.
License activation error by (Errore di attivazione licenza di): *Utente*	Visualizza la data e l'ora in cui si verifica un errore durante l'attivazione della licenza.
iLO 2 RBSU user login (Accesso utente RBSU iLO 2): *Utente*	Visualizza la data e l'ora in cui un utente autorizzato accede all'utility RBSU di iLO 2.
Power on request received by (Richiesta di accensione ricevuta da): *Tipo*	È stata ricevuta una richiesta di accensione dei tipi seguenti: Funzione Power Button Attivazione LAN Accensione automatica
Virtual NMI selected by (NMI virtuale selezionato da): *Utente*	Visualizza la data e l'ora in cui un utente autorizzato seleziona il pulsante NMI virtuale.
Virtual Serial Port session started by: (Sessione porta seriale virtuale avviata da:) *Utente*	Visualizza la data e l'ora in cui è stata avviata una sessione della porta seriale virtuale.
Virtual Serial Port session stopped by (Sessione porta seriale virtuale interrotta da): *Utente*	Visualizza la data e l'ora in cui è terminata una sessione della porta seriale virtuale.
Virtual Serial Port session login failure from (Errore di accesso sessione porta seriale virtuale da): *Utente*	Visualizza la data e l'ora in cui si è verificato un errore di accesso per una sessione della porta seriale virtuale.

Problemi relativi ai collegamenti hardware e software

iLO 2 utilizza cavi Ethernet standard, tra cui CAT5 UTP con connettori RJ-45. Questi cavi sono necessari per stabilire un collegamento hardware a un hub Ethernet standard. Per un collegamento diretto al PC, utilizzare un cavo incrociato.

È necessario collegare la porta di gestione di iLO 2 a una rete, che a sua volta deve essere collegata a un server DHCP. Prima di accendere il sistema, iLO 2 deve essere già disponibile in rete. DHCP invia una richiesta subito dopo l'attivazione dell'alimentazione. Se al primo avvio di iLO 2 la richiesta DHCP non riceve risposta, continua a essere inviata a intervalli di 90 secondi.

Il server DHCP deve essere configurato per fornire la risoluzione dei nomi DNS e WINS. iLO 2 può essere configurato per il funzionamento con un indirizzo IP statico nell'impostazione della ROM tramite l'opzione F8 o nella pagina Web Network Settings (Impostazioni di rete).

Il nome DNS predefinito è riportato sull'etichetta delle impostazioni di rete e può essere utilizzato per individuare iLO 2 quando non si conosce l'indirizzo IP assegnato.

In caso di collegamento diretto a un PC, è necessario utilizzare un indirizzo IP statico poiché sul collegamento non è presente alcun server DHCP.

Nell'utility RBSU di iLO 2 è possibile premere il tasto **F1** nella pagina DNS/DHCP per accedere alle opzioni avanzate e visualizzare lo stato delle richieste DHCP di iLO 2.

Supporto di JVM

Per assicurarsi che le applet della console remota di iLO 2 e dei supporti virtuali funzionino come previsto, è opportuno installare Java Runtime Environment, Standard Edition 1.4.2_13. Per individuare un collegamento alla versione più recente supportata di JRE, dall'interfaccia del browser di iLO 2 selezionare **Remote Console>Settings>Java** (Console remota>Impostazioni>Java).

Per l'esecuzione delle applet della console remota di iLO 2, della console seriale remota e dei supporti virtuali è necessario che sul server sia installato JVM. Se si accede alle applet della console remota e dei supporti virtuali utilizzando una versione di Java™ Runtime Environment Standard Edition successiva alla 1.4.2_13, è possibile che queste non funzionino correttamente. Se si utilizza un'altra versione di JVM, possono verificarsi le situazioni illustrate di seguito.

- Se l'applet della console remota viene aperta con Java™ Runtime Environment versione 1.5.x o 1.6.x, può verificarsi quanto segue:
  - Viene visualizzato il messaggio "Automation server cannot create object" (Il server di automazione non è in grado di creare l'oggetto). Se si fa clic su **OK**, il messaggio scompare e l'applet funziona normalmente.
  - Il tasto TAB non funziona correttamente, ovvero si sposta nelle varie parti della finestra dell'applet, anziché all'interno dell'applet stessa.
- Se l'applet Virtual Media viene aperta con Java™ Runtime Environment versione 1.5.x o 1.6.x, può verificarsi quanto segue:
  - Quando si fa clic sul pulsante **Create Disk Image** (Crea immagine disco), viene visualizzata un'altra finestra. È possibile che in questa finestra non siano presenti i pulsanti Create (Crea) e Cancel (Annulla) o che venga visualizzato solo testo. Se si chiude e si riapre la finestra, i pulsanti verranno visualizzati correttamente.
  - Quando si seleziona un file di immagine nell'applet, viene visualizzata una finestra per la selezione dei file. Dopo la selezione di un file, questa finestra viene chiusa e viene nuovamente visualizzata la normale finestra dell'applet. Tuttavia, l'area del file di immagine non viene aggiornata e l'applet sembra non rispondere. Per aggiornare la finestra dell'applet dei supporti virtuali originale e consentire a tale finestra di mantenere lo stato di attivazione nel sistema, fare clic su una finestra separata. L'applet non risulta in grado di rispondere finché la finestra dell'applet dei supporti virtuali non viene chiusa e riaperta.

Problemi di accesso

Per tentare di risolvere i problemi di accesso, usare le seguenti informazioni:

- Provare ad avviare la modalità di accesso predefinito, disponibile nella scheda delle impostazioni di rete.
- Se l'utente dimentica la password, un amministratore con privilegio Administer User Accounts (Amministra account utente) può reimpostarla.

- Se un amministratore dimentica la propria password, deve usare la funzione Security Override Switch (Interruttore di esclusione della protezione) o definire un account amministratore e una password mediante HPONCFG.
- Verificare la presenza di problemi standard rispondendo alle seguenti domande:
  - La password è conforme alle relative restrizioni? La password contiene caratteri che fanno distinzione tra maiuscole e minuscole?
  - Il browser utilizzato non è supportato?

Nome di accesso e password non accettati

Se è stata effettuata la connessione a iLO 2 ma la password e il nome di accesso non vengono accettati, è necessario verificare che le informazioni di accesso siano configurate correttamente. Richiedere l'intervento di un utente che disponga del privilegio di Administer User Accounts (Amministra account utente) per accedere e modificare la password. Se il problema persiste, chiedere all'utente di accedere di nuovo, eliminare l'account utente e aggiungerlo nuovamente.

NOTA: È possibile eseguire l'utility RBSU anche per correggere i problemi di accesso.

Disconnessione anomala dell'utente di directory

Gli errori di rete possono causare la conclusione anomala della connessione alla directory. Se iLO 2 non è in grado di rilevare la directory, la connessione alla directory verrà interrotta. Gli eventuali tentativi di accesso aggiuntivi alla connessione interrotta causano il reindirizzamento del browser alla pagina di accesso.

Il reindirizzamento alla pagina di accesso potrebbe essere interpretato come un timeout anomalo della sessione. Durante una sessione attiva, è possibile che si verifichi il timeout anomalo della sessione se:

- Il traffico della connessione di rete è intenso.
- Il server di directory è spento.

Per ripristinare il sistema in caso di timeout anomalo della sessione, effettuare nuovamente l'accesso e continuare a utilizzare iLO 2. Se il server di directory non è disponibile, è necessario utilizzare un account locale.

Impossibilità di accedere alla porta di gestione di iLO 2 per nome

La porta di gestione di iLO 2 può essere registrata con un server WINS o un server DDNS per risolvere i nomi in indirizzi IP al fine di accedere alla porta di gestione di iLO 2 per nome. Prima di alimentare la porta di gestione di iLO 2, è necessario che sia in esecuzione un server WINS o DDNS. La porta, inoltre, deve disporre di un percorso di instradamento valido al server WINS o DDNS.

La porta di gestione di iLO 2 deve infine essere configurata con l'indirizzo IP del server WINS o DDNS. È possibile utilizzare il protocollo DHCP per configurare il server DHCP con gli indirizzi IP necessari, nonché immettere gli indirizzi IP tramite l'utility RBSU o l'opzione **Network Settings** (Impostazioni di rete) nella scheda Administration (Amministrazione). La porta di gestione di iLO 2 deve essere configurata per la registrazione con un server WINS o DDNS. Queste opzioni sono predefinite in fabbrica e possono essere modificate tramite l'utility RBSU o selezionando **Network Settings** (Impostazioni di rete) nella scheda Administration (Amministrazione).

I client usati per accedere alla porta di gestione di iLO 2 devono essere configurati per usare lo stesso server DDNS con cui è stato registrato l'indirizzo IP della porta di gestione di iLO.

Se si utilizza un server WINS e un server DNS non dinamico, l'accesso alla porta di gestione di iLO 2 è notevolmente più rapido se il server DNS viene configurato in modo da utilizzare il server WINS per

la risoluzione dei nomi. Per ulteriori informazioni, consultare la documentazione Microsoft® corrispondente.

Utility RBSU di iLO 2 non disponibile in seguito alla reimpostazione del server e di iLO 2

Se il server viene reimpostato subito dopo la reimpostazione del processore iLO 2, il firmware di iLO 2 potrebbe non essere reinizializzato completamente durante l'inizializzazione del server e il tentativo di richiamo dell'utility RBSU di iLO 2. In questo caso, l'utility non sarà disponibile o il codice della ROM opzionale di iLO 2 verrà completamente ignorato. In tal caso, ripristinare di nuovo il server. Per evitare che il problema si ripresenti, attendere alcuni secondi prima di reimpostare il server dopo la reimpostazione del processore iLO 2.

Impossibilità di collegarsi alla pagina di accesso

Se non è possibile collegarsi alla pagina di accesso, verificare il livello di codifica SSL del browser sia impostato a 128 bit. Il livello di codifica SSL in iLO 2 è impostato a 128 bit e non può essere modificato. I livelli di codifica del browser e di iLO 2 devono corrispondere.

Impossibilità di accedere a iLO 2 mediante Telnet

Se non è possibile accedere a iLO 2 tramite Telnet, verificare la configurazione della porta e la codifica dei dati della console remota nella schermata Global Settings (Impostazioni globali). Se la configurazione della porta della console remota è impostata su Automatic (Automatico), l'applet della console remota abilita la porta 23 e avvia una sessione al termine della quale la porta viene chiusa. Poiché non può abilitare automaticamente la porta 23, Telnet rileva un errore.

Impossibilità di accedere alla console grafica remota o ai supporti virtuali

I supporti virtuali e la console grafica remota sono attivi solo se si dispone di una licenza di iLO Advanced Pack opzionale. Un messaggio informa l'utente che le funzioni non sono disponibili in mancanza di questa licenza. Anche se 10 utenti possono accedere contemporaneamente a iLO 2, un solo utente alla volta può accedere alla console remota. Un messaggio di avvertenza informerà che la console remota è già occupata.

Impossibilità di collegarsi a iLO 2 dopo la modifica delle impostazioni di rete

Verificare che le due parti del collegamento, il controller di rete e il dispositivo, presentino le stesse impostazioni per la selezione automatica della velocità del ricetrasmettitore, la velocità e il duplex. Ad esempio, se una parte è impostata sulla selezione automatica del collegamento, l'altra deve essere impostata nello stesso modo. Le impostazioni del controller di rete di iLO 2 sono contenute nella schermata Network Settings (Impostazioni di rete).

Impossibilità di collegarsi alla porta di diagnostica di iLO 2

Se non è possibile effettuare il collegamento alla porta di diagnostica di iLO 2 tramite il controller di rete, tenere presente quanto segue:

- L'uso della porta di diagnostica viene rilevato automaticamente quando si collega un cavo di rete attivo. Quando si passa dalle porte posteriori alle porte di diagnostica, attendere per un minuto la conclusione del processo di commutazione della rete prima di tentare una nuova connessione mediante il browser Web.
- Se è in corso un'attività critica, la porta di diagnostica non può essere utilizzata fino alla conclusione di questa attività. Le attività critiche comprendono:
  - Aggiornamento del firmware
  - Sessione della console remota
  - Inizializzazione SSL
- Se si utilizza una workstation client che contiene più di un controller di rete abilitato, ad esempio una scheda wireless e una scheda di rete, un problema di instradamento potrebbe impedire l'accesso alla porta di diagnostica. Per risolvere questo problema:

1. Verificare che sulla workstation client sia attivo un solo controller di rete. Ad esempio, disabilitare la scheda di rete wireless.
2. Configurare l'indirizzo IP della rete in cui si trova la workstation client in base alla rete della porta di diagnostica di iLO 2, in modo da soddisfare le seguenti condizioni:
   - L'impostazione dell'indirizzo IP è 192.168.1.*X*, dove la *X* è un numero diverso da 1 poiché l'indirizzo IP impostato per la porta di diagnostica è 192.168.1.1.
   - L'impostazione della maschera di sottorete è 255.255.255.0.

Impossibilità di stabilire il collegamento al processore iLO 2 tramite la scheda di interfaccia di rete

Se non è possibile stabilire il collegamento al processore iLO 2 tramite il controller di rete (NIC), eseguire una o tutte le operazioni di risoluzione descritte di seguito:

- Verificare che sul connettore iLO 2 RJ-45 sia accesa la luce verde dell'indicatore LED (stato del collegamento), Questa condizione indica che il collegamento tra la scheda NIC PCI e l'hub di rete è corretto.
- Verificare che la luce verde dell'indicatore LED lampeggi in modo intermittente, a indicare un traffico di rete normale.
- Eseguire l'utility RBSU di iLO 2 per accertarsi che il controller di rete sia abilitato e verificare l'indirizzo IP e la maschera di sottorete assegnati.
- Eseguire l'utility RBSU di iLO 2 e utilizzare la scheda F1 – Advanced (F1 – Avanzate) della pagina DNS/DHCP per visualizzare lo stato delle richieste DHCP.
- Eseguire il ping dell'indirizzo IP del controller di rete da una workstation di rete separata.
- Tentare di stabilire la connessione con il software del browser digitando l'indirizzo IP del controller di rete come URL. Da questo indirizzo è possibile visualizzare la home page di iLO 2.
- Reimpostare iLO 2.

NOTA: Se si stabilisce una connessione di rete, è necessario attendere per 90 secondi la ricezione della richiesta del server DHCP.

I server ProLiant BL p-Class dispongono di una porta di diagnostica. Se si collega alla porta di diagnostica un cavo di rete attivo, il processore iLO 2 passa automaticamente dalla porta iLO 2 alla porta di diagnostica. Quando si passa dalle porte posteriori alle porte di diagnostica, attendere per un minuto la conclusione del processo di commutazione della rete prima di tentare una nuova connessione mediante il browser Web.

Impossibilità di accedere a iLO 2 dopo l'installazione del certificato

Se il certificato con firma automatica di iLO 2 è installato in modo permanente in alcuni browser e si reimposta iLO 2, potrebbe non essere possibile accedere nuovamente a iLO 2 poiché viene generato un nuovo certificato con firma automatica ogni volta che iLO 2 viene reimpostato. Quando si installa un certificato nel browser, viene indicizzato con il nome contenuto nel certificato. Questo nome è univoco per ciascun processore iLO 2. Ogni volta che iLO 2 viene reimpostato, viene generato un nuovo certificato con lo stesso nome.

Per evitare questo problema, non installare il certificato con firma automatica iLO 2 nell'archivio certificati del browser. Se si desidera installare il certificato di iLO 2, è necessario richiedere un certificato permanente a una CA e importarlo nel processore iLO 2. Tale certificato può essere quindi installato nell'archivio certificati del browser.

Problemi relativi al firewall

iLO 2 comunica tramite porte TCP/IP configurabili. Se sono bloccate, l'amministratore deve configurare il firewall per consentire la comunicazione su tali porte. Per visualizzare o modificare le configurazioni delle porte, vedere la sezione Administration (Amministrazione) dell'interfaccia utente di iLO 2.

Problemi relativi al server proxy

Se il software del browser Web è configurato per l'utilizzo di un server proxy, non è possibile connettersi all'indirizzo IP di iLO 2. Per risolvere questo problema, configurare il browser in modo da non utilizzare il server proxy per l'indirizzo IP di iLO 2. In Internet Explorer, ad esempio, selezionare **Strumenti>Opzioni Internet>Connessioni>Impostazioni LAN>Avanzate**, quindi inserire il nome DNS o l'indirizzo IP di iLO 2 nel campo Eccezioni.

Errori nell'autenticazione basata su due fattori

Quando si tenta di autenticare iLO 2 utilizzando l'autenticazione basata su due fattori, è possibile che venga visualizzato il messaggio `The page cannot be displayed` (Impossibile visualizzare la pagina). Questo messaggio viene visualizzato nei casi seguenti:

- Sul sistema client non è stato registrato alcun certificato utente. Per correggere questo problema, registrare il certificato utente appropriato sul sistema client, utilizzando, se necessario, il software fornito con la smart card.
- Il certificato utente è memorizzato in una smart card o in un'unità USB non collegata al sistema client. Per correggere questo problema, collegare la smart card o l'unità USB appropriata al sistema client.
- Il certificato utente non è stato rilasciato da una CA attendibile. Il certificato di una CA attendibile deve essere configurato in iLO 2 nella pagina delle impostazioni relative all'autenticazione basata su due fattori. Il certificato configurato come certificato di una CA attendibile deve essere il certificato pubblico della CA che emette certificati all'interno della propria organizzazione. Per correggere questo problema, configurare il certificato appropriato come certificato di una CA attendibile nella pagina delle impostazioni relative all'autenticazione basata su due fattori oppure utilizzare un certificato utente rilasciata dalla CA attendibile già configurata.

- Il certificato utente è scaduto oppure non è ancora valido. iLO 2 non consente di effettuare l'autenticazione con un certificato scaduto o non ancora valido, indipendentemente dal fatto che questo sia associato a un account utente locale o a un account utente di directory. Controllare il periodo di validità del certificato per verificare se possa costituire il motivo per cui viene visualizzato il messaggio `The page cannot be displayed` (Impossibile visualizzare la pagina). Per correggere questo problema, fornire all'utente un certificato valido. Associare il certificato all'account utente iLO 2 locale se si sta effettuando l'autenticazione di utenti iLO 2 locali e verificare che l'orologio di iLO 2 sia impostato correttamente.
- La firma digitale del certificato utente non corrisponde al certificato specificato come CA attendibile. Anche se il nome riportato sul certificato della CA attendibile coincide con l'ente che ha emesso il certificato utente, la firma digitale del certificato utente può corrispondere a un certificato diverso. Verificare il percorso di certificazione relativo al certificato utente per verificare che la chiave pubblica del certificato emesso sia la stessa del certificato della CA attendibile. Per correggere questo problema, configurare il certificato appropriato come certificato di una CA attendibile nella pagina delle impostazioni relative all'autenticazione basata su due fattori oppure utilizzare un certificato utente rilasciata dalla CA attendibile.

Risoluzione dei problemi relativi a trap e allarmi

Allarme	Descrizione
Test Trap (Trap di prova)	Questo trap viene generato da un utente mediante la pagina di configurazione Web.
Server Power Outage (Mancanza di alimentazione del server)	L'alimentazione del server è insufficiente.
Server Reset (Reimpostazione del server)	Il server è stato reimpostato.
Failed Login Attempt (Tentativo di accesso non riuscito)	Il tentativo di accesso utente in remoto non è riuscito.
General Error (Errore generico)	Si è verificata una condizione di errore non predefinita dal MIB a codifica hardware.
Logs (Registri)	Il registro circolare è stato sovraccaricato.
Security Override Switch Changed (Interruttore di esclusione della protezione modificato): On/Off (Attivato/Disattivato)	Lo stato dell'interruttore è stato modificato (On/Off)
Rack Server Power On Failed (Accensione server rack non riuscita)	Il server non si è acceso e il rack BL p-Class ha segnalato la presenza di un'alimentazione insufficiente ad avviare la procedura di accensione.
Rack Server Power On Manual Override (Accensione manuale del server rack)	Il server è stato acceso manualmente malgrado la segnalazione di alimentazione insufficiente del rack BL p-Class.
Rack Name Changed (Nome rack modificato)	Il nome del rack ProLiant BL p-Class è stato modificato.

Impossibilità di ricevere allarmi di HP SIM (allarmi SNMP) da iLO 2

Per poter configurare i parametri dei trap SNMP, l'utente che dispone del privilegio Configure iLO 2 Settings (Configura impostazioni iLO 2) deve accedere a iLO 2. Una volta stabilita la connessione a iLO 2, è necessario verificare che nella schermata SNMP/Insight Manager Settings (Impostazioni SNMP/Insight Manager) della console di iLO 2 siano stati abilitati i tipi di allarme e le destinazioni dei trap corretti.

Interruttore di esclusione della protezione di iLO 2

L'attivazione dell'interruttore di esclusione della protezione di iLO 2 consente all'amministratore di eseguire l'accesso di emergenza per controllare fisicamente la scheda di sistema del server. L'impostazione di questo interruttore permette di accedere con tutti i privilegi senza dover immettere l'ID utente e la password.

L'interruttore di esclusione della protezione di iLO 2 si trova sul server e non è possibile accedervi senza aprire il contenitore del server. Per impostare l'interruttore di esclusione della protezione di iLO 2 è necessario spegnere il server e scollegarlo dall'alimentazione. Impostare quindi l'interruttore e riaccendere il server. Eseguire la procedura in senso inverso per disattivare l'interruttore di esclusione della protezione di iLO 2.

Nelle pagine Web di iLO 2 viene visualizzato un messaggio di avvertenza che indica che l'interruttore di esclusione della protezione è in uso. Nel registro di iLO 2 viene aggiunta una voce relativa all'uso di questo interruttore. Anche quando si attiva o si disattiva l'interruttore di esclusione della protezione di iLO 2 potrebbe venire inviato un allarme SNMP.

Se necessario, è possibile attivare l'interruttore di esclusione della protezione di iLO 2 per aggiornare il blocco di avvio di iLO 2. Il blocco di avvio rimane esposto fino alla reimpostazione di iLO 2. HP consiglia di scollegare iLO 2 dalla rete fino al completamento della reimpostazione.

A seconda del server, l'interruttore di esclusione della protezione di iLO 2 può essere un singolo ponticello o una posizione di interruttore specifica su un pannello di microinterruttori. Per accedere all'interruttore, consultare la documentazione del server.

Messaggio di errore relativo al codice di autenticazione

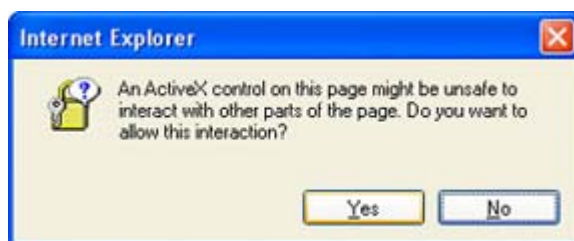
Quando si utilizza il browser Mozilla, è possibile che venga visualizzato un messaggio improprio di errore relativo al codice di autenticazione che segnala l'avvenuta modifica della coppia di chiavi pubblica o privata e del certificato utilizzati per avviare la sessione SSL del browser. Questo messaggio di errore può essere visualizzato quando non si usa un certificato fornito dal cliente, poiché a ogni avvio iLO 2 genera un proprio certificato con firma automatica.

Per risolvere il problema, chiudere il browser Web e riavviarlo, oppure installare i propri certificati in iLO 2.

Risoluzione dei problemi relativi alle directory

Nelle sezioni seguenti vengono descritte le procedure di risoluzione dei problemi relativi alle directory.

Problemi relativi all'accesso con il formato dominio/nome

Per accedere utilizzando il formato dominio/nome, è necessario che siano attivati i controlli ActiveX. Per verificare che il browser consenta che lo script di accesso richiami i controlli ActiveX, aprire Internet Explorer e impostare i controlli ActiveX su **Prompt**. Dovrebbe essere visualizzata una figura simile a quella riportata di seguito.

I controlli ActiveX sono abilitati e la finestra di richiesta di conferma è visualizzata, ma il formato dominio/nome non funziona

1. Accedere con un account locale e determinare il nome del server di directory.
2. Verificare che il nome del server di directory sia effettivamente un nome e non un indirizzo IP.
3. Verificare che sia possibile eseguire il ping del nome del server di directory da parte del client in uso.
4. Eseguire le verifiche della configurazione delle directory. Verificare che il ping sia stato ricevuto in modo corretto. Per ulteriori informazioni sulle verifiche delle impostazioni delle directory, vedere la sezione "Verifiche di directory" (Verifiche di directory a pagina 53).

I contesti utente non funzionano

Controllare con l'amministratore della rete. Il nome distinto completo dell'oggetto utente deve essere presente nella directory. Il nome di accesso è quello visualizzato dopo il primo CN=. La parte rimanente del nome distinto dovrebbe essere visualizzata in uno dei campi del contesto utente. Per i contesti utente non viene effettuata la distinzione tra maiuscole e minuscole. In ogni caso, qualsiasi altro elemento, compresi gli spazi, fa parte del contesto utente.

L'utente della directory non è in grado di disconnettersi in seguito al timeout della directory

Se si imposta il timeout di iLO 2 su Infinite (Infinito), la console remota effettua periodicamente il ping del firmware per verificare la presenza di una connessione. Durante questa operazione, il firmware di iLO 2 invia alla directory una richiesta di autorizzazioni utente. L'invio di una richiesta a intervalli regolari mantiene attiva la connessione della directory, impedendo il timeout e consentendo l'accesso dell'utente.

Risoluzione dei problemi relativi alla console remota

Nelle sezioni seguenti vengono descritte le procedure di risoluzione dei problemi relativi alla console remota. In genere:

- Programmi di blocco delle finestre a comparsa impediscono l'avvio della console remota e della porta seriale virtuale.
- Le applicazioni di blocco delle finestre a comparsa impostate per impedire l'apertura automatica di nuove finestre impediscono l'esecuzione della console remota e della porta seriale virtuale. Prima di avviare la console remota o la porta seriale virtuale, disabilitare tutti i programmi di blocco delle finestre a comparsa.

Sull'applet della console remota compare una X rossa quando è in esecuzione un browser del client Linux

È necessario configurare i browser Mozilla in modo che accettino i cookie.

1. Aprire il menu Preferences (Preferenze) e selezionare **Privacy & Security>Cookies** (Privacy e Sicurezza>Cookie).
2. Nella schermata Level of Privacy (Livello di privacy), selezionare **Allow cookies based on privacy settings** (Accetta cookie in base alle impostazioni di privacy), quindi fare clic su **View** (Visualizza).
3. Nella schermata Cookies (Cookie), selezionare **Allow cookies based on privacy settings** (Accetta cookie in base alle impostazioni di privacy).

È necessario che il livello di privacy sia impostato su medio o basso.

Impossibilità di spostare il cursore negli angoli della finestra della console remota

Talvolta non è possibile spostare il cursore del mouse negli angoli della finestra della console remota. In questi casi, fare clic con il pulsante destro del mouse per trascinare il cursore all'esterno della finestra, quindi di nuovo all'interno.

Se il mouse continua a non funzionare correttamente o questo problema si verifica di frequente, controllare che le impostazioni del mouse corrispondano a quelle consigliate nella sezione "Ottimizzazione delle prestazioni del mouse per la console remota o la console remota integrata" (Ottimizzazione delle prestazioni del mouse per la console remota o la console remota integrata a pagina 95).

Console remota non più aperta nella sessione del browser esistente

Con l'aggiunta della funzione pass-through di Servizi terminal, il comportamento dell'applet della console remota risulta leggermente diverso rispetto alle precedenti versioni del firmware di iLO 2. Se è già aperta una sessione della console remota e si seleziona di nuovo il collegamento della console remota, la sessione non verrà avviata e la sessione della console remota potrebbe apparire bloccata.

Questo accade quando, ad esempio, si eseguono le seguenti operazioni:

1. Accesso a iLO 2 dal Client-1 e apertura di una sessione della console remota.
2. Accesso a iLO 2 dal Client-2 e tentativo di apertura di una sessione della console remota. Verrà visualizzato il messaggio `Remote console is already opened by another session` (La console remota è stata già aperta da un'altra sessione). Si tratta del funzionamento previsto poiché la console remota supporta solo una sessione alla volta.
3. Ritorno al Client-1 e chiusura della sessione della console remota.
4. Dal Client-2, selezione del collegamento della console remota con l'applet della console remota precedente già aperta. Non verrà aggiornata la sessione della console remota e apparirà di nuovo il messaggio di cui al punto 2.

Si tratta del funzionamento previsto con questa versione del firmware di iLO, sebbene sia diverso rispetto alle precedenti versioni del firmware di iLO. Per evitare che si verifichino problemi di questo genere, chiudere e aprire la sessione della console remota prima di aprirla di nuovo.

Aggiornamento non corretto della finestra di testo della console remota

Se si utilizza la console remota per visualizzare le finestre di testo a scorrimento veloce, la finestra potrebbe non essere aggiornata in modo corretto. Questo errore è dovuto ad aggiornamenti di schermate troppo veloci che non vengono rilevati e visualizzati dal firmware di iLO 2. In genere viene aggiornato solo l'angolo in alto a sinistra della finestra di testo, mentre il resto della finestra rimane invariato. Al termine dello scorrimento, fare clic su **Refresh** (Aggiorna) per aggiornare in modo corretto la finestra di testo.

Questa situazione si verifica, ad esempio, durante l'avvio di Linux e l'esecuzione del POST; in questo caso, alcuni messaggi POST possono andare perduti. Una possibile conseguenza è la richiesta di una risposta della tastiera durante la procedura di avvio. Tale risposta va comunque perduta. Per evitare questo problema, le procedure di avvio e di POST devono essere rallentate nello script di avvio di Linux in modo da aumentare il tempo di risposta della tastiera.

Lo schermo della console remota diventa grigio o nero

Lo schermo della console remota diventa grigio o nero quando il server viene riavviato dal client di Servizi terminal. Lo schermo resterà grigio o nero per un minino di 30 secondi e un massimo di 1 minuto. Il server di Servizi terminal non sarà disponibile ed effettuerà la chiusura del client. La console remota di iLO 2 sarà operativa, ma lo schermo diventerà grigio o nero. Quando viene ripristinato il normale stato dello schermo, sarà possibile usare normalmente la console remota.

Risoluzione dei problemi relativi alla console seriale remota

L'opzione Remote Serial Console (Console seriale remota) dipende dalla funzione Virtual Serial Port (Porta seriale virtuale). La porta seriale virtuale deve essere correttamente abilitata e configurata nell'utility RBSU del server host. È possibile accedere alla porta seriale virtuale mediante SSH o Telnet (se abilitato). Se il dispositivo UART e la porta seriale virtuale hanno le stesse impostazioni, è possibile accedere a CLP da una sessione seriale dell'host. Per effettuare questa operazione, digitare **Esc(** (senza parentesi sinistra) per passare all'interprete della riga di comando.

Le applicazioni di blocco delle finestre a comparsa impediranno l'esecuzione dell'opzione Remote Serial Console (Console seriale remota). Prima di avviare la console seriale remota, disabilitare tutti i programmi di blocco delle finestre a comparsa.

Risoluzione dei problemi relativi alla console remota integrata

Per la console remota integrata possono verificarsi i seguenti problemi:

- Problemi di interazione con Internet Explorer 7
- Necessità di configurare il server Web Apache per l'esportazione
- Nessuna riproduzione su console quando il server è spento
- Perdita di informazioni durante la riproduzione dei buffer di avvio e degli errori

Sfarfallio dello schermo della console remota con Internet Explorer 7

L'utilizzo di Internet Explorer 7 con lo schermo della console remota può causare un problema di sfarfallio e rendere difficile la lettura dei dati. Per ridurre lo sfarfallio è possibile impostare l'accelerazione hardware del sistema su un livello inferiore. Per modificare il livello di accelerazione hardware, selezionare **Pannello di controllo>Schermo**, quindi selezionare la scheda **Impostazioni** e fare clic su **Advanced** (Avanzate). Quando viene visualizzata la finestra delle proprietà avanzate, selezionare la scheda **Risoluzione problemi**. Ridurre il livello di **Accelerazione hardware** finché non scompare lo sfarfallio.

Configurazione di Apache per i buffer di acquisizione esportati

Per consentire la corretta esecuzione della funzionalità Console Replay Export (Esportazione dati riproduzione console), è necessario configurare un server Web in modo da accettare i dati dei buffer. Di seguito è riportato un esempio delle modifiche da apportare alla configurazione di Apache versione 2.0.59(Win32) su un server con sistema operativo Microsoft Windows Server™ 2003.

È necessario selezionare un percorso in cui memorizzare i dati esportati, impostare le autorizzazioni di Apache per la scrittura in questo percorso e configurare l'autenticazione. Per effettuare quest'ultima operazione, è necessario eseguire `htpasswd.exe` in modo da creare nomi utente e password per l'autenticazione ad Apache quando viene ricevuta una richiesta di accesso al percorso di esportazione.

Per ulteriori informazioni sulla configurazione degli utenti, visitare il sito Web Apache Software Foundation (http://httpd.apache.org/docs/2.0/howto/auth.html).

WebDAV fornisce un ambiente di collaborazione per la modifica e la gestione dei file sui server Web. In termini tecnici, DAV è un'estensione del protocollo http. È necessario apportare modifiche al file di configurazione per consentire a WebDAV di caricare i moduli di supporto per gli oggetti dinamici condivisi. In particolare, è necessario aggiungere due righe all'elenco dei moduli nel file `http.conf`, ovvero `LoadModule dav_module modules/mod_dav.so` e `LoadModule dav_fs_module modules/mod_dav_fs.so`.

È inoltre necessario abilitare l'autenticazione caricando i moduli `LoadModule auth_module modules/mod_auth.so, LoadModule auth_digest_module modules/mod_auth_digest.so`.

Se non è presente una directory per il database DavLock, è necessario crearne una. A questo scopo è sufficiente creare una directory DAV in Apache2, a cui viene fatto riferimento nel file di configurazione. Di seguito è riportato un esempio di modifiche da apportare a `http.conf` per aggiungere questo supporto:

```
# Davlock database location
DavLockDb "C:/apache/Apache2/Apache2/dav/davlock"
# location of data being exported
Alias /images/ "C:/images/"
# Configuration of the directory to support PUT Method with authentication
<Directory "C:/images">
AllowOverride FileInfo AuthConfig Limit
AuthType Digest
# if digest is not supported by your configuration use the following
# AuthType Basic
# location of the usernames and passwords used for authentication
AuthUserFile "C:/Program Files/apache group/Apache2/passwd/passwords"
# specifies the user that is required for authentication, can be a group
# For group change to the following after creating the appropriate group
# Require group GroupName
Require user Administrator
Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
Dav On
<Limit GET PUT OPTIONS PROPFIND>
Order allow,deny
Allow from all
</Limit>
</Directory>
```

Nessuna riproduzione su console quando il server è spento

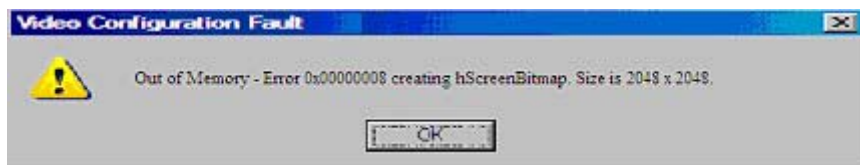
La riproduzione dei buffer di acquisizione e delle sessioni di console registrate non è disponibile quando il server è spento. È possibile riprodurre i buffer acquisiti esportandoli su un server Web e riproducendo i file sulla console remota integrata di un altro server. Per effettuare questa operazione, esportare manualmente il buffer con il pulsante di esportazione disponibile nella pagina Remote Console>Settings (Console remota>Impostazioni) dopo aver configurato il server Web e il percorso di esportazione.

Perdita di informazioni durante la riproduzione dei buffer di avvio e degli errori

La perdita di informazioni sullo schermo è un problema che accade normalmente e può essere riscontrato durante la riproduzione dei buffer di avvio e degli errori. Per limitare questo problema,

assicurarsi che la console remota integrata sia attiva durante l'avvio e la registrazione degli errori. Se si continua a riscontrare una perdita di dati, provare ad acquisire manualmente queste sequenze. Per effettuare questa operazione, avviare la console remota integrata e fare clic sul pulsante per la registrazione.

Errore di memoria insufficiente durante l'avvio della console remota integrata

Se vengono aperte contemporaneamente troppe sessioni di console remota integrata, è possibile che sul sistema client si verifichi un errore di memoria insufficiente. Ogni sessione di console remota integrata richiede almeno 16 MB di memoria per lo spazio del buffer dello schermo e la funzionalità relativa alla cartella virtuale può utilizzare circa 100 MB. Se durante l'avvio della console remota integrata viene visualizzato un messaggio, significa che sul client non è disponibile una quantità di memoria sufficiente per il buffering dei dati dello schermo. Ad esempio:

Per correggere questi tipi di errore, chiudere alcune sessioni di console remota integrata oppure aggiungere memoria al computer client per consentire l'apertura simultanea di un numero maggiore di sessioni.

Mancata ricezione delle richieste di connessione da parte del responsabile di sessione quando la console remota integrata è in modalità di riproduzione

Quando il responsabile della sessione esegue la riproduzione dei dati di acquisizione video, è possibile che non riceva il messaggio di avviso `Deny or Accept` (Nega o Accetta) in caso di tentativo di accesso o condivisione della console remota integrata da parte di un altro utente. La nuova sessione rimarrà in attesa fino a generare un errore di timeout. Se si richiede l'accesso alla console remota integrata, si tenta di accedere e viene generato un errore di timeout, utilizzare la funzionalità Acquire (Acquisisci) per acquisire il controllo della console.

Visualizzazione non corretta del LED della tastiera

Il LED della tastiera del client non riflette lo stato effettivo dei vari tasti di blocco della tastiera. Tuttavia, i tasti BLOC MAIUSC, BLOC NUM e BLOC SCORR sono pienamente funzionanti quando si utilizza l'opzione Key Up/Down (Tastiera attivata/disattivata) nella console remota integrata.

Console remota integrata inattiva

Durante i periodi di elevata attività è possibile che la console remota integrata di iLO 2 diventi inattiva o venga disconnessa. Il problema è indicato dallo stato inattivo della console. Prima del passaggio allo

stato inattivo, si verifica un rallentamento dell'attività della console. Di seguito sono indicati i possibili sintomi di questo problema:

- Il display della console remota integrata non viene aggiornato.
- L'attività della tastiera e del mouse non viene registrata.
- Le richieste della console remota condivisa non vengono registrate.
- La connessione Virtual Media visualizza un dispositivo di supporto virtuale vuoto.

Anche se è possibile riprodurre un file acquisito su una console remota integrata inattiva, lo stato attivo della console non viene ripristinato.

Il problema può verificarsi quando più utenti sono connessi a iLO 2, una sessione Virtual Media è connessa e sta eseguendo un'operazione di copia continua oppure una sessione della console remota integrata è aperta. L'operazione di copia continua della sessione Virtual Media ha priorità e, di conseguenza, la console remota integrata perde la sincronizzazione. Alla fine, la connessione Virtual Media viene reimpostata più volte, causando la perdita di sincronizzazione dell'unità USB del sistema con il client Virtual Media.

Per ovviare a questo problema, riconnettersi alla console remota integrata e a Virtual Media. Se possibile, ridurre il numero di connessioni utente simultanee a iLO 2 ed eventualmente reimpostare iLO 2 (non è necessario reimpostare il server).

Messaggio di errore relativo alla connessione della console remota integrata al server

Durante il tentativo di stabilire una sessione di console remota integrata, è possibile che iLO 2 restituisca il messaggio `Failed to connect to server` (Impossibile connettersi al server). Verificare una connessione Telnet disponibile.

Il client della console remota integrata di iLO 2 attende per un determinato periodo di tempo che venga stabilita una connessione tra la console e iLO 2. Se il server non riceve risposta entro il tempo specificato, viene restituito un messaggio di errore.

Di seguito sono indicate le possibili cause di questo messaggio:

- Si verificano ritardi nei tempi di risposta di rete.
- È stata richiesta una sessione di console remota condivisa, ma il responsabile di sessione ritarda a inviare un messaggio di rifiuto o accettazione.

Per ovviare a questo problema, ritentare la connessione della console remota integrata. Se possibile, correggere il ritardo della rete e ritentare la connessione della console. Se è stata effettuata una richiesta di sessione di console remota condivisa, provare a contattare il responsabile della sessione e ritentare la richiesta. Se la funzione di acquisizione della console remota è abilitata, utilizzare il pulsante Acquire (Acquisisci) anziché richiedere una sessione di console remota condivisa.

Mancato aggiornamento delle icone della barra degli strumenti della console remota integrata

Quando si stabilisce una connessione alla console remota integrata su iLO 2 versione 1.30, nel browser viene installato un oggetto IRC (applet della console remota di iLO 2). Questo oggetto include le icone della barra degli strumenti per le nuove funzionalità incluse in iLO 2 versione 1.30. Quando si accede a iLO 2 versione 1.29 o precedente, l'oggetto IRC non viene sostituito dalla versione inclusa nel firmware precedente. Di conseguenza, sulla barra degli strumenti vengono visualizzate le icone relative a funzionalità incluse nella versione 1.30 di iLO 2 che non sono disponibili nelle versioni precedenti. Se si fa clic su un'icona, viene visualizzato un messaggio di errore.

Per rimuovere manualmente l'oggetto IRC:

1. Da un browser Microsoft® Internet Explorer 6, fare clic su **Strumenti>Opzioni Internet**.
2. Selezionare **File temporanei Internet>Impostazioni**.
3. Fare clic su **Visualizza oggetti**.
4. Fare clic con il pulsante destro del mouse su **iLO 2 Remote Console Applet** e scegliere **Rimuovi**.
5. Fare clic su **OK** per rimuovere l'oggetto, quindi di nuovo su **OK** per chiudere.

Impossibilità di blocco dell'interfaccia GNOME

Quando il processore iLO 2 e l'interfaccia GNOME sono configurati per la funzionalità di blocco della console remota, l'interruzione di una console remota iLO 2 o la perdita della connettività di rete iLO 2 non determina il blocco dell'interfaccia GNOME.

Il gestore di tastiera GNOME richiede tempo per elaborare sequenze di tasti che contengono modificatori. Questo comportamento non si verifica quando le sequenze di tasti vengono immesse manualmente tramite la console remota integrata, ma può costituire un problema quando la sequenza di tasti viene inviata da iLO 2, poiché in questo caso la velocità di invio della sequenza è superiore a quella di elaborazione del gestore di tastiera GNOME.

Per ovviare a questo problema, in alternativa a GNOME è possibile utilizzare la GUI KDE di Linux. Il gestore di tasti KDE, infatti, non richiede un'eccessiva quantità di tempo per elaborare le sequenze di tasti contenenti modificatori. Entrambe le interfacce KDE e GNOME vengono fornite con tutte le distribuzioni di Linux.

Ripetizione di tasti sulla console remota

Quando si utilizza la console remota in determinate condizioni di latenza di rete, è possibile registrare più pressioni di tasto per un'unica pressione. Per ulteriori informazioni, vedere la sezione "Impostazioni della console remota" (Impostazioni della console remota a pagina 87).

Mancata riproduzione su console remota quando il server host è spento

In caso di collegamento a un server host spento, la riproduzione su console remota non viene eseguita. Per accedere ai file della console remota registrati, accendere il server o collegarsi a un altro processore iLO 2 su un server acceso.

Risoluzione dei problemi relativi a SSH e Telnet

Nelle sezioni seguenti vengono descritte le procedure di risoluzione dei problemi relativi a SSH e Telnet.

Input inizialmente lento di PuTTY

Durante la connessione iniziale mediante un client PuTTY, l'input viene accettato lentamente per circa 5 secondi. Questo problema può essere risolto nelle opzioni di configurazione nel client nelle opzioni di connessione Low-level TCP (Basso livello di TCP), deselezionando l'opzione **Disable Nagle's algorithm** (Disabilita algoritmo di Nagle). Nelle opzioni relative a Telnet, impostare Telnet Negotiation Mode (Modalità di negoziazione Telnet) su **Passive** (Passiva).

Il client PuTTY non risponde con la porta di rete condivisa

Quando si usa il client PuTTY con la porta di rete condivisa, è possibile che la sessione PuTTY non risponda quando si trasferisce una grande quantità di dati o si utilizzano una porta seriale virtuale e una console remota. Per risolvere il problema, chiudere il client PuTTY, quindi riavviare la sessione.

Supporto del testo SSH da una sessione di console remota

L'accesso a Telnet e SSH dalla console remota a interfaccia testo supporta la configurazione standard 80 x 25 dello schermo di testo. Questa modalità è compatibile con la console remota per la maggior parte delle interfacce in modalità testo disponibili negli attuali sistemi operativi. Una configurazione del testo superiore al formato 80 x 25 non viene visualizzata correttamente quando si usano Telnet e SSH. HP consiglia di configurare l'applicazione di testo nella modalità 80 x 25 o di usare l'applet della console remota di iLO 2 inclusa nell'interfaccia Web.

Risoluzione dei problemi relativi a Servizi terminal

Nelle sezioni seguenti vengono descritte le procedure di risoluzione dei problemi relativi a Servizi terminal.

Pulsante di Servizi terminal non funzionante

L'opzione Servizi terminal non è operativa se nella finestra di avviso protezione di Java è selezionata l'opzione Deny (Nega), poiché il browser considererà l'applet della console remota come non attendibile. Non sarà possibile eseguire la console remota e l'eventuale codice con richiesta di attendibilità di livello superiore. Se l'opzione Deny (Nega) è selezionata, non sarà possibile avviare sulla console remota il codice richiesto per attivare il pulsante di Servizi terminal. Sulla console Java verrà visualizzato il messaggio "`Security Exception - Access denied`" (Eccezione di protezione – Accesso negato).

Mancata risposta del proxy di Servizi terminal

Ogni volta che iLO 2 viene reimpostato (ad esempio se si modificano le impostazioni di rete o le impostazioni globali), la funzione pass-through di Servizi terminal non è disponibile per due minuti dall'inizio della reimpostazione. iLO 2 richiede 60 secondi per eseguire la reimpostazione e il test POST più un buffer di 60 secondi prima di continuare. Dopo due minuti, lo stato diventa disponibile ed è possibile utilizzare la funzione pass-through di Servizi terminal.

Risoluzione dei problemi relativi a schermi e monitor

Nelle sezioni seguenti vengono descritti i fattori da tenere in considerazione per la risoluzione dei problemi relativi a schermi e monitor.

Istruzioni generali

- La risoluzione dello schermo del client deve essere maggiore di quella del server remoto.
- La console remota di iLO 2 supporta solo il chip video ATI Rage XL integrato nel sistema. Se si installa una scheda video plug-in, non sarà disponibile la funzionalità console remota di iLO 2, ma solo le altre funzionalità di iLO 2.
- Alla console remota può accedere un solo utente alla volta. Verificare se un utente è già connesso a iLO 2.

Visualizzazione non corretta di Telnet in DOS®

Se si utilizza la sessione Telnet di iLO 2 per visualizzare le schermate di testo con una finestra DOS® ingrandita e se lo schermo del server ha dimensioni maggiori di 80 x 25, risulta visibile solo la parte superiore della schermata.

Per correggere questo errore, impostare le proprietà delle finestre di DOS® in modo da limitarne le dimensioni a 80 x 25 prima di ingrandirle.

- Nella barra del titolo della finestra DOS®, fare clic con il pulsante destro del mouse e selezionare **Proprietà**, quindi **Layout**.
- Nella scheda Layout, per Dimensioni buffer dello schermo impostare l'altezza su 25.

Applicazioni video non visualizzate nella console remota

Alcune applicazioni video, ad esempio Microsoft® Media Player, non vengono visualizzate nella console remota o vengono visualizzate in modo non corretto. Questo problema si riscontra soprattutto nelle applicazioni che utilizzano registri di sovrapposizione video. In genere, le applicazioni video utilizzano questo tipo di registri. iLO 2 non è progettato per essere usato con questo tipo di applicazione.

Interfaccia utente non visualizzata correttamente

Nei server ProLiant che utilizzano iLO 2 con Red Hat EL 4.0 o altri sistemi operativi Linux, il testo sui pulsanti dell'interfaccia utente potrebbe non risultare interamente visualizzato nella parte inferiore. Questo errore si verifica perché Mozilla Firefox non supporta le dimensioni di testo specificate da iLO 2 per i pulsanti dell'interfaccia utente. Per visualizzare correttamente il testo, selezionare **View>Text Size>Decrease** (Visualizza>Dimensioni testo>Riduci) finché il testo non appare interamente leggibile.

Risoluzione dei problemi relativi ai supporti virtuali

Nelle sezioni seguenti vengono descritte le procedure di risoluzione dei problemi relativi ai supporti virtuali.

Applet Virtual Media non visualizzata perché associata a una X rossa

L'applet Virtual Media può generare una X rossa se si usa una versione non supportata del browser o di JVM, o se l'opzione Enable All Cookies (Abilita tutti i cookie) non è abilitata. Per correggere il problema, accertarsi di usare una versione supportata del browser e di JVM sul client, analizzando la relativa tabella nella sezione "Browser e sistemi operativi client supportati" (Browser e sistemi operativi client supportati a pagina 6). Verificare inoltre che l'opzione Enable All Cookies (Abilita tutti i cookie) sia selezionata nel menu Preferenze o Opzioni del browser. Per impostazione predefinita alcuni browser non abilitano i cookie.

L'applet del dischetto virtuale non risponde

Se il dischetto fisico contiene degli error, è possibile che l'applet del dischetto virtuale di iLO 2 non risponda.

Per evitare che l'applet del dischetto virtuale non risponda, eseguire CHKDSK.EXE (o una utility simili) per controllare gli errori del dischetto fisico. Se il supporto fisico contiene degli errori, ricaricare l'immagine del dischetto su un nuovo dischetto fisico.

Risoluzione di problemi del riproduttore video iLO

Nelle sezioni seguenti vengono descritte le procedure di risoluzione dei problemi relativi ai iLO Video Player (Riproduttore video iLO).

Il file di acquisizione video non funziona

Verificare che sia un file di acquisizione per HP iLO 2 valido e non sia danneggiato.

Il file di acquisizione funziona in modo discontinuo

I file di acquisizione di iLO 2 registrano le attività in corso sullo schermo. Durante lunghi periodi di inattività dello schermo, l'operazione di registrazione viene interrotta per ridurre la dimensione del file e migliorare le prestazioni di riproduzione. Questo potrebbe dar luogo alla discontinuità di riproduzione.

Risoluzione dei problemi relativi alla console di testo remota

Nelle sezioni seguenti vengono descritti i fattori da tenere in considerazione per la risoluzione dei problemi relativi alla console di testo remota.

Visualizzazione del file di installazione di Linux nella console di testo

Quando si installa Linux utilizzando la console di testo, la schermata di installazione iniziale non viene visualizzata perché lo schermo è in modalità grafica. Per correggere il problema e procedere con l'installazione, effettuare una delle seguenti operazioni:

- Per la maggior parte delle versioni Linux, digitare `linux text nofb`. I caratteri immessi non verranno visualizzati. Se il comando viene inserito correttamente, lo schermo passa dalla modalità grafica alla modalità di testo, visualizzando così la schermata di installazione.
- Per le versioni SLES 9 e SLES 10, premere **F2** e ↓ (freccia giù) dalla console di testo. In questo modo viene attivata la modalità di testo e visualizzata la scherma di installazione.

Passaggio di dati mediante un terminale SSH

Se si utilizza un terminale SSH per accedere alla console di testo, SSH potrebbe intercettare i dati relativi alle sequenze di tasti e non passarli alla console di testo. Ne consegue che la sequenza di tasti non sembra produrre il risultato previsto. Per correggere questo problema, disabilitare qualsiasi operazione di scelta rapida mediante terminale SSH.

Risoluzione di problemi vari

Nelle sezioni che seguono vengono descritte le procedure per la risoluzione di problemi hardware o software di varia natura.

Condivisione di cookie tra le istanze del browser e iLO 2

iLO 2 utilizza i cookie della sessione del browser per distinguere accessi separati (ciascuna finestra del browser viene visualizzata come un singolo accesso utente), pur condividendo la stessa sessione attiva di iLO 2. Questi molteplici accessi possono confondere il browser. Tale confusione potrebbe sembrare un problema di iLO 2. In realtà, si tratta di un comportamento tipico del browser.

Diversi processi possono causare l'apertura di finestre aggiuntive del browser. Le finestre del browser aperte all'interno del browser in esecuzione rappresentano i differenti aspetti dello stesso programma all'interno della memoria. Di conseguenza, ciascuna finestra del browser condivide le proprietà con la finestra principale, inclusi i cookie.

Istanze condivise

Quando iLO 2 apre un'altra finestra del browser, ad esempio la finestra della console remota, dei supporti virtuali o della Guida, questa condivide la stessa connessione a iLO 2 e il cookie della sessione.

Il server Web di iLO 2 prende le decisioni relative all'URL in base a ciascuna richiesta ricevuta. Ad esempio, una richiesta priva di diritti di accesso verrà reindirizzata in qualsiasi caso alla pagina di accesso. Se si esegue un reindirizzamento basato su server Web, selezionando **File>New>Window** (File>Nuovo>Finestra) o premendo la sequenza di tasti **Ctrl+N**, viene aperta un'istanza duplicata del browser originale.

Funzionamento dell'ordine dei cookie

Durante l'accesso, la pagina di accesso crea un cookie della sessione del browser che collega la finestra alla sessione appropriata nel firmware. Il firmware registra gli accessi del browser come sessioni distinte elencate nella sezione Active Sessions (Sessioni attive) della pagina di stato di iLO 2.

Ad esempio, quando l'Utente1 effettua l'accesso, il server Web crea la visualizzazione della finestra iniziale con il nome utente corrente: Utente1 nel pannello superiore, le voci di menu nel pannello sinistro e i dati della pagina nel pannello inferiore destro. Quando l'Utente1 seleziona i vari collegamenti, vengono aggiornate solo le voci di menu e i dati della pagina.

Se mentre l'Utente1 è collegato, un altro utente, ad esempio Utente2, apre un'altra finestra del browser nello stesso client ed effettua l'accesso, il secondo accesso sovrascriverà il cookie generato nella sessione dell'Utente1. Supponendo che l'Utente2 disponga di un account utente diverso, verrà creata una finestra corrente differente e verrà consentito l'accesso alla nuova sessione. La seconda sessione verrà visualizzata nella sezione Active Sessions (Sessioni attive) della pagina di stato di iLO 2 come utente corrente: Utente2.

Il secondo accesso ha in pratica reso orfana la prima sessione (Utente1) cancellando il cookie generato durante l'accesso dell'Utente1. Lo stesso funzionamento si registra quando il browser dell'Utente1 viene chiuso senza selezionare il collegamento Log Out (Disconnessione). La sessione orfana dell'Utente1 verrà recuperata allo scadere del timeout della sessione.

La finestra dell'utente corrente viene aggiornata solo se al browser viene imposto l'aggiornamento dell'intera pagina, pertanto l'Utente1 sarà in grado di proseguire la navigazione utilizzando la propria finestra del browser. Il browser tuttavia utilizza attualmente le impostazioni del cookie relative alla sessione dell'Utente2, sebbene ciò non risulti evidente.

Se l'Utente1 prosegue la navigazione in questa modalità (Utente1 e Utente2 che condividono lo stesso processo poiché l'Utente2 ha effettuato l'accesso e reimpostato il cookie della sessione), potrebbero verificarsi le seguenti condizioni:

- La sessione dell'Utente1 viene svolta con i privilegi assegnati all'Utente2.
- L'attività dell'Utente1 mantiene attiva la sessione dell'Utente2, ma può verificarsi il timeout inaspettato della sessione dell'Utente1.
- La disconnessione da tutte le finestre causa la chiusura di entrambe le sessioni. L'attività successiva nell'altra finestra può causare il reindirizzamento dell'utente alla pagina di accesso, come in caso di timeout della sessione o timeout anomalo.
- Se si seleziona Log Out (Disconnessione) nella seconda sessione (Utente2), viene visualizzato il messaggio `Logging out: unknown page to display before redirecting the`

`user to the login page.` (Disconnessione: pagina sconosciuta da visualizzare prima del reindirizzamento dell'utente alla pagina di accesso).

- Se l'Utente2 si scollega e si collega di nuovo come Utente3, l'Utente1 assumerà la sessione dell'Utente3.
- Se l'Utente1 effettua l'accesso mentre l'Utente2 è già collegato, l'Utente1 potrà modificare l'URL per il reindirizzamento alla pagina dell'indice. Sembra che l'Utente1 abbia effettuato l'accesso a iLO 2 senza collegarsi.

Tale funzionamento viene ripetuto finché sono aperte finestre duplicate. Tutte le attività verranno attribuite allo stesso utente, utilizzando l'insieme di cookie della sessione più recente.

Visualizzazione del cookie della sessione corrente

Dopo l'accesso, è possibile imporre al browser di visualizzare il cookie della sessione corrente immettendo `javascript:alert(document.cookie)` nella barra di navigazione degli indirizzi URL. Il primo campo visibile è costituito dall'ID di sessione. Se diverse finestre del browser utilizzano lo stesso ID di sessione, tali finestre condividono la stessa sessione iLO 2.

Per imporre al browser l'aggiornamento e la visualizzazione della reale identità di un utente, premere il tasto **F5**, selezionare **View**>**Refresh** (Visualizza>Aggiorna) oppure utilizzare il pulsante di aggiornamento.

Prevenzione dei problemi dell'utente relativi ai cookie

Per prevenire che si verifichino problemi associati ai cookie:

- Avviare un nuovo browser per ciascun accesso facendo clic sull'icona del browser o sul collegamento.
- Prima di chiudere la finestra del browser, fare clic sul collegamento **Log Out** (Disconnessione) per chiudere la sessione di iLO 2.

Impossibilità ad accedere ai download di ActiveX

Se la rete utilizzata non consente i controlli ActiveX, è possibile acquisire il file DVC.DLL da un singolo sistema e distribuirlo ai client collegati in rete.

1. Accedere a iLO 2.
2. Digitare **https://iLO_name/dvc.cab** nella barra degli indirizzi del browser.
3. Viene visualizzata la finestra di download del file. Fare clic su **Apri** e salvare il file DVC.DLL sul disco locale.
4. Copiare il file DVC.DLL sul sistema client che non consente il download di ActiveX.
5. Da questo client, aprire una finestra di prompt dei comandi. Spostarsi sulla directory contenente il file DVC.DLL e digitare `regsvr32 dvc.dll`.

Impossibilità di ottenere informazioni SNMP da HP SIM

Gli agenti in esecuzione sul server gestito forniscono informazioni SNMP a HP SIM. Affinché gli agenti siano in grado di trasmettere le informazione tramite iLO 2, è necessario che siano installati i driver di iLO 2. Per istruzioni sull'installazione, vedere la sezione "Installazione dei driver di iLO 2".

Se i driver e gli agenti per iLO sono stati installati, verificare che iLO e il PC di gestione si trovino sulla stessa sottorete. La verifica può essere eseguita rapidamente effettuando il ping di iLO 2 dal PC di

gestione. Per conoscere i percorsi di instradamento validi per accedere all'interfaccia di rete di iLO 2, rivolgersi all'amministratore.

Ora o data errate delle voci del registro eventi

iLO 2 supporta l'aggiornamento della data e dell'ora tramite l'utility RBSU, che imposta automaticamente per il processore la data e l'ora del server. Questi valori vengono inoltre aggiornati da Insight Management Agents sui sistemi operativi di rete supportati.

Impossibilità di aggiornare il firmware di iLO 2

Se si tenta di aggiornare il firmware di iLO 2 ma il processore non risponde, non accetta l'aggiornamento del firmware o l'aggiornamento non viene completato, è possibile ripristinare il firmware di iLO 2 utilizzando una delle opzioni riportate di seguito. Per informazioni dettagliate sull'utilizzo delle funzionalità di scripting di iLO 2, consultare la Guida delle risorse mediante la riga di comando e lo scripting di iLO 2.

- **Aggiornamento firmware online** - Scaricare questo componente ed eseguirlo dall'amministratore o dal contesto radice di un sistema operativo supportato. Il software viene eseguito sul sistema operativo host e aggiorna il firmware di iLO 2 senza che sia necessario accedere a iLO 2.
- **Aggiornamento del firmware offline per il CD di manutenzione SmartStart** - Scaricare il componente da utilizzare con il CD di manutenzione del firmware SmartStart dalla sezione ROM Update Utility (Utility di aggiornamento della ROM) della scheda Maintenance (Manutenzione). Questi componenti possono essere utilizzati anche con l'utility HP Drive Key Boot (Avvio da chiave HP).
- **CD di manutezione del firmware** - Scaricare il componente per creare un CD-ROM di avvio contenente numerosi aggiornamenti del firmware per le opzioni e i server ProLiant.
- **Scripting con CPQLOCFG** - Scaricare l'utility di scripting basata su rete CPQLOCFG. CPQLOCFG consente di utilizzare in modo sicuro attraverso la rete gli script RIBCL per l'esecuzione degli aggiornamenti del firmware, la configurazione di iLO 2 e altre operazioni in blocco relative a iLO 2. Gli utenti Linux possono esaminare gli esempi di script in XML e PERL per HP Lights-Out.
- **Scripting con HPONCFG** - Scaricare l'utility di scripting basata su host, HPONCFG. Questa utility consente di utilizzare script RIBCL per l'esecuzione degli aggiornamenti del firmware, la configurazione del processore LOM e di altre operazioni in blocco usando un account che dispone dei privilegi di accesso alla directory principale o dell'amministratore sui sistemi operativi host.
- **HP Directories Support for Management Processors** - Scaricare questa utility per disporre dei componenti di supporto delle directory. Uno dei componenti, HPLOMIG, può essere utilizzato per rilevare i processori iLO, iLO 2, RILOE e RILOE II e aggiornare il relativo firmware. Per usufruire di questa funzionalità non è necessario utilizzare l'integrazione delle directory.

Procedure di diagnostica

Prima di tentare il recupero della riprogrammazione del firmware, eseguire le seguenti procedure di diagnostica per accertarne la reale necessità:

1. Tentare di collegarsi a iLO 2 tramite il browser Web. Se non è possibile effettuare il collegamento significa che si è verificato un problema di comunicazione.
2. Tentare di eseguire il ping di iLO 2. Se questa operazione può essere effettuata, la rete funziona correttamente.

Mancata risposta di iLO 2 alle richieste SSL

iLO 2 non risponde alle richieste SSL quando è visualizzato un avviso Java™. Se un utente tenta di accedere a una connessione browser di iLO 2 senza completare la procedura di accesso rispondendo all'avviso di certificato Java, iLO 2 non risponderà alle future richieste del browser. L'utente deve continuare la procedura di accesso per liberare il server Web di iLO 2.

Verifica di SSL

Il seguente test verifica la corretta finestra di dialogo di protezione visualizzata. Un server non funzionante causa la visualizzazione del messaggio `Page cannot be displayed` (Impossibile visualizzare la pagina). Se l'esito del test è negativo, significa che il controller di dominio non accetta le connessioni SSL e probabilmente non è stato emesso alcun certificato.

1. Avviare un browser e accedere all'indirizzo <https://<*controller dominio*>:636.

   È possibile sostituire <*dominio*> a <*controller dominio*>, che punta al DNS e verifica quale controller di dominio sta gestendo le richieste per il dominio. Verificare più controller di dominio per sapere se per tutti è stato emesso un certificato.

2. Se SSL funziona correttamente sul controller di dominio (è stato emesso un certificato), mediante un messaggio sulla protezione viene chiesto se si intende continuare la procedura di accesso al sito o si preferisce visualizzare il certificato del server. Facendo clic su **Sì** non viene visualizzata alcuna pagina Web. Si tratta di un comportamento normale. La procedura è automatica, ma può richiedere il riavvio. Per evitare il riavvio:

   a. Aprire MMC e aggiungere lo snap-in dei certificati. Quando richiesto, selezionare **Account del computer** per il tipo di certificato che si desidera visualizzare. Fare clic su **OK** per tornare allo snap-in dei certificati.

   b. Selezionare la cartella **Personale>Certificati**. Fare clic con il pulsante destro del mouse sulla cartella e selezionare **Richiedi nuovo certificato**.

   c. Verificare che Tipo sia un controller di dominio, quindi fare clic su **Avanti** finché non viene usato un certificato.

Per verificare le connessioni SSL è inoltre possibile usare lo strumento LDP di Microsoft®. Per ulteriori informazioni sullo strumento LDP, visitare il sito Web Microsoft® (http://www.microsoft.com/support).

Un certificato obsoleto può causare problemi con SSL sul controller di dominio quando punta a un'autorità di certificazione considerata precedentemente attendibile con lo stesso nome. Ciò è raro ma può capitare se un servizio di certificati viene aggiunto, rimosso, quindi aggiunto di nuovo sul controller di dominio. Per rimuovere i certificati obsoleti e emetterne uno nuovo, seguire le istruzioni di cui al punto 2.

Reimpostazione di iLO 2

In casi rari, può essere necessario reimpostare iLO 2, ad esempio se non risponde al browser. Per eseguire questa operazione è necessario spegnere il server e scollegarlo completamente dall'alimentazione.

In alcuni casi iLO 2 esegue una reimpostazione automatica. Se il firmware rileva un problema in iLO 2, ad esempio, un timer watchdog interno di iLO 2 viene reimpostato automaticamente. iLO 2 si reimposta anche dopo il completamento dell'aggiornamento del firmware o dopo la modifica di un'impostazione di rete.

Utilizzando HP Insight Management Agents 5.40 o versioni successive, è possibile reimpostare iLO 2. Per reimpostare iLO 2, effettuare una delle seguenti operazioni:

- Selezionare l'opzione **Reset** (Reimposta) per iLO 2 nella sezione iLO 2 della pagina Web HP Management Agent.
- Fare clic su **Apply** (Applica) nella pagina Network Settings (Impostazioni di rete) per avviare manualmente il processo di reimpostazione del processore di gestione iLO 2. Prima di fare clic su Apply (Applica) non è necessario aver modificato alcun parametro.
- Fare clic su **Reset** (Reimposta) nella pagina Diagnostic (Diagnostica) dell'interfaccia del browser di iLO 2.

Nome del server ancora presente dopo l'esecuzione della utility ERASE

Il contenuto del campo Server Name (Nome server) viene comunicato a iLO 2 mediante gli agenti Insight Manager.

Per rimuovere il campo Server Name (Nome server) in seguito alla reinstallazione di un server, effettuare una delle seguenti operazioni:

- Caricare gli Insight Manager Agents per aggiornare il contenuto del campo con il nuovo nome del server.
- Utilizzare la funzionalità Reset to Factory Defaults (Ripristina valori predefiniti) dell'utility RBSU di iLO 2 per cancellare il campo Server Name (Nome server).

  Oltre all'informazione sul nome del server, questa procedura cancella tutte le informazioni di configurazione di iLO 2.
- Modificare il nome del server nella pagina Administration>Access>Options (Amministrazione>Accesso>Opzioni) dell'interfaccia del browser di iLO 2.

Risoluzione dei problemi di un host remoto

Per risolvere i problemi di un server host remoto può essere necessario riavviare il sistema remoto, mediante le opzioni disponibili nella scheda Virtual Devices (Dispositivi virtuali).

10 Schema dei servizi di directory

In questa sezione

Attributi e classi OID LDAP principali della gestione HP

Le modifiche apportate allo schema durante il processo di configurazione dello schema includono la modifica di:

- Classi principali (Classi principali a pagina 233)
- Attributi principali (Attributi principali a pagina 233)

Classi principali

Nome classe	OID assegnato
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Attributi principali

Nome attributo	OID assegnato
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Definizione delle classi principali

Nella seguente tabella sono definite le classi principali di gestione HP.

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1

Descrizione	Questa classe definisce gli oggetti Destinazione e fornisce la basi per i prodotti HP che utilizzano la gestione abilitata alla directory.
Tipo di classe	Strutturale
Superclasse	Utente
Attributi	hpqPolicyDN – 1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership – 1.3.6.1.4.1.232.1001.1.1.2.2
Note	Nessuno

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Descrizione	Questa classe definisce gli oggetti Ruolo e fornisce la basi per i prodotti HP che utilizzano la gestione abilitata alla directory.
Tipo di classe	Strutturale
Superclasse	Gruppo
Attributi	hpqRoleIPRestrictions – 1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault – 1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction – 1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership – 1.3.6.1.4.1.232.1001.1.1.2.3
Note	Nessuno

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Descrizione	Questa classe definisce gli oggetti Criterio e fornisce la basi per i prodotti HP che utilizzano la gestione abilitata alla directory.
Tipo di classe	Strutturale
Superclasse	Superiore
Attributi	hpqPolicyDN – 1.3.6.1.4.1.232.1001.1.1.2.1
Note	Nessuno

Definizioni degli attributi principali

Nella seguente tabella sono definiti gli attributi delle classi principali di gestione HP.

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1

Descrizione	Nome distinto del criterio che controlla la configurazione generale di questa destinazione.
Sintassi	Nome distinto – 1.3.6.1.4.1.1466.115.121.1.12
Opzioni	A valore singolo
Note	Nessuno

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Descrizione	Fornisce un elenco degli oggetti hpqTarget ai quali appartiene questo oggetto.
Sintassi	Nome distinto – 1.3.6.1.4.1.1466.115.121.1.12
Opzioni	A valore multiplo
Note	Nessuno

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Descrizione	Fornisce un elenco di oggetti hpqTarget che appartengono a questo oggetto.
Sintassi	Nome distinto – 1.3.6.1.4.1.1466.115.121.1.12
Opzioni	A valore multiplo
Note	Nessuno

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Descrizione	Una valore booleano che rappresenta l'accesso da client non specificati che definisce parzialmente le restrizioni dei diritti in base a una restrizione dell'indirizzo IP corrente.
Sintassi	Booleano – 1.3.6.1.4.1.1466.115.121.1.7
Opzioni	A valore singolo
Note	Se questo attributo è TRUE, le restrizioni IP verranno soddisfatte per i client di rete non eccezionali. Se questo attributo è FALSE, le restrizioni IP non verranno soddisfatte per i client di rete non eccezionali.

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5

Descrizione	Fornisce un elenco di indirizzi IP, nomi DNS, domini, intervalli di indirizzi e sottoreti che specificano parzialmente le restrizioni dei diritti in base a una restrizione dell'indirizzo IP di rete.
Sintassi	Stringa ottetto – 1.3.6.1.4.1.1466.115.121.1.40
Opzioni	A valore multiplo
Note	Questo attributo viene utilizzato solo per gli oggetti ruolo. Le restrizioni IP vengono soddisfatte quando l'indirizzo corrisponde e l'accesso generale è negato. Non vengono soddisfatte quando l'indirizzo corrisponde e l'accesso generale è consentito. I valori sono costituiti da un byte identificativo seguito da un numero di tipo specifico o byte che specificano un indirizzo di rete. • Per le sottoreti IP, l'identificativo è <0x01>, seguito dall'indirizzo IP di rete secondo l'ordine di rete, seguito dalla maschera di sottorete della rete IP secondo l'ordine della rete. Ad esempio, la sottorete IP 127.0.0.1/255.0.0.0 verrebbe rappresentata come <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. Per gli intervalli IP, l'identificativo è <0x02>, seguito dall'indirizzo IP associato più basso, seguito dall'indirizzo IP associato più alto. Sono entrambi inclusivi e in ordine di rete, ad esempio, l'intervallo IP da 10.0.0.1 a 10.0.10.255 verrebbe rappresentato come <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>. • Per i nomi DNS o domini, l'identificativo è <0x03>, seguito dal nome DNS codificato ASCII. Ai nomi DNS è possibile aggiungere il prefisso * (ASCII 0x2A), per indicare che devono corrispondere a tutti i nomi che terminano con la stringa specificata. Ad esempio il dominio DNS *.acme.com viene rappresentato come <0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. È consentito l'accesso generale.

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Descrizione	Una griglia oraria di sette giorni, con incrementi di 30 minuti, che specifica le restrizioni dei diritti in base a un vincolo temporale.
Sintassi	Stringa ottetto {42} – 1.3.6.1.4.1.1466.115.121.1.40
Opzioni	A valore singolo
Note	Questo attributo viene utilizzato solo con gli oggetti RUOLO.

	Le restrizioni temporali vengono soddisfatte quando il bit corrispondente all'ora effettiva del proprio paese per il dispositivo è 1 e non vengono soddisfatte quanto il bit è 0. ● Il bit meno significativo del primo byte corrisponde a domenica, dalle ore 24.00 alle 12.30. ● Tutti i bit meno significativi e il byte seguente corrispondono ai successivi blocchi di mezz'ora della settimana. ● Il bit più significativo (8°) e il 42° bit corrispondono alla fascia oraria compresa tra le ore 23.30 di sabato e le 24.00 di domenica.

Attributi e classi OID LDAP specifici della gestione Lights-Out

I seguenti attributi e classi dello schema potrebbero dipendere dalle classi o dagli attributi principali definiti per la gestione HP.

Classi di gestione Lights-Out

Nome classe	OID assegnato
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Attributi di gestione Lights-Out

Nome classe	OID assegnato
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.1
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.6

Definizione delle classi di gestione Lights-Out

La seguente tabella definisce le classi principali di gestione Lights-Out.

hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Descrizione	Questa classe definisce i Diritti e le Impostazioni utilizzati con i prodotti di gestione Lights-Out.
Tipo di classe	Ausiliaria

Superclasse	Nessuno
Attributi	hpqLOMRightConfigureSettings – 1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin – 1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin – 1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole – 1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset – 1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia – 1.3.6.1.4.1.232.1001.1.8.2.6
Note	Nessuno

Definizione degli attributi di gestione Lights-Out

Nella seguente tabella sono definiti gli attributi delle classi principali di gestione di Lights-Out.

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Descrizione	Diritto di accesso per i prodotti di gestione HP Lights-Out.
Sintassi	Booleano – 1.3.6.1.4.1.1466.115.121.1.7
Opzioni	A valore singolo
Note	Significativo solo con gli oggetti RUOLO. Se TRUE, i membri del ruolo dispongono del diritto.

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Descrizione	Diritto della console remota per i prodotti di gestione Lights-Out. Significativo solo con gli oggetti RUOLO.
Sintassi	Booleano – 1.3.6.1.4.1.1466.115.121.1.7
Opzioni	A valore singolo
Note	Questo attributo viene utilizzato solo con gli oggetti RUOLO. Se è TRUE, i membri del ruolo dispongono del diritto.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Descrizione	Diritto dei supporti virtuali per i prodotti di gestione HP Lights-Out.
Sintassi	Booleano – 1.3.6.1.4.1.1466.115.121.1.7

Opzioni	A valore singolo
Note	Questo attributo viene utilizzato solo con gli oggetti RUOLO. Se è TRUE, i membri del ruolo dispongono del diritto.

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Descrizione	Diritto di reimpostazione remota del server e diritto del pulsante di accensione per i prodotti di gestione HP Lights-Out.
Sintassi	Booleano – 1.3.6.1.4.1.1466.115.121.1.7
Opzioni	A valore singolo
Note	Questo attributo viene utilizzato solo con gli oggetti RUOLO. Se è TRUE, i membri del ruolo dispongono del diritto.

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Descrizione	Diritto di amministrazione del database utente locale per i prodotti di gestione HP Lights-Out.
Sintassi	Booleano – 1.3.6.1.4.1.1466.115.121.1.7
Opzioni	A valore singolo
Note	Questo attributo viene utilizzato solo con gli oggetti RUOLO. Se è TRUE, i membri del ruolo dispongono del diritto.

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Descrizione	Diritto di configurazione delle impostazioni dei dispositivi per i prodotti di gestione HP Lights-Out.
Sintassi	Booleano – 1.3.6.1.4.1.1466.115.121.1.7
Opzioni	A valore singolo
Note	Questo attributo viene utilizzato solo con gli oggetti RUOLO. Se è TRUE, i membri del ruolo dispongono del diritto.

11 Assistenza tecnica

In questa sezione

Informazioni relative al supporto

HP iLO Advanced Pack e HP iLO Advanced Pack for BladeSystem, forniti di serie con le suite Insight Control e con iLO Power Management Pack, includono un servizio di assistenza tecnica e aggiornamento software fornito da HP per un anno. Questo servizio fornisce l'accesso alle risorse tecniche HP per facilitare la risoluzione dei problemi di funzionamento o implementazione del software, nonché l'accesso agli aggiornamenti software e ai manuali di riferimento resi disponibili da HP in formato elettronico o su supporti fisici.

HP offre servizi di supporto e aggiornamento dei prodotti per i clienti di HP iLO Advanced e HP iLO Advanced Pack for BladeSystem nei due modi descritti di seguito.

- Se vengono acquistate licenze individuali, viene fornito il supporto telefonico gratuito per la fase di implementazione iniziale, entro 90 giorni dalla data di acquisto. Contattando il servizio di assistenza telefonica, è possibile richiedere informazioni sull'installazione e sulla configurazione, nonché formulare domande sugli script predefiniti e sul relativo utilizzo. I numeri per contattare il servizio di assistenza HP nel mondo sono disponibili sul sito Web HP (http://www.hp.com/country/us/en/support.html). Gli aggiornamenti possono essere acquistati anche separatamente.
- Se HP iLO Advanced Pack e HP iLO Advanced Pack for BladeSystem vengono ottenuti con l'acquisto di una suite Insight Control o di iLO Power Management Pack, le licenze includono un servizio di aggiornamento e assistenza tecnica software per un anno.

  Con questo nuovo servizio di aggiornamento e assistenza tecnica, i clienti di HP iLO Advanced Pack e HP iLO Advanced Pack for BladeSystem potranno beneficiare del supporto per la risoluzione rapida dei problemi, nonché delle funzionalità dinamiche di notifica e consegna degli aggiornamenti software di iLO Advanced e iLO Select. Per ulteriori informazioni, visitare il sito Web HP (http://www.hp.com/go/iLO), selezionare il prodotto e consultare la sezione sulle specifiche tecniche.

  Per attivare il servizio di aggiornamento e assistenza tecnica software fornito da HP per iLO Advanced e iLO Select, è necessario effettuare la registrazione del proprio acquisto software sul sito Web HP (http://www.hp.com/go/iLO). **In caso di mancata registrazione, il servizio non viene attivato**.

  Dopo la registrazione, all'utente viene assegnato un SAID (Service Agreement Identifier). Una volta ottenuto questo ID, l'utente può accedere alla pagina Web SUM (Software Update Manager) per visualizzare il contratto e scegliere la consegna elettronica, oltre agli aggiornamenti standard sul supporto. Per ulteriori informazioni su questo servizio, visitare il sito Web HP (http://www.hp.com/services/insight).

HP offre anche servizi di supporto software aggiuntivi, molti dei quali vengono forniti gratuitamente.

- Supporto telefonico gratuito per l'implementazione iniziale – Fornisce il supporto telefonico per le operazioni di installazione, configurazione e avvio del prodotto. Questo servizio viene fornito da personale specializzato nelle soluzioni HP Insight Control Management e HP Systems Insight Manager ed è disponibile gratuitamente per 90 giorni dalla data di acquisto del server. Per richiedere assistenza negli Stati Uniti, chiamare il numero:
- 1-800-HP-INVENT (1-800-474-6836). (Quando richiesto, pronunciare "Insight Manager, P2P o SMP".) I numeri di supporto per contattare il servizio di assistenza HP nel mondo sono disponibili sul sito Web HP (http://www.hp.com/country/us/en/wwcontact.html).
- Partecipazione alla discussione (http://forums.itrc.hp.com) – Il forum relativo al supporto HP è uno strumento basato su una comunità di utenti realizzato in modo che i clienti HP possano scambiare informazioni e idee sui prodotti HP. Per limitare la discussione alle soluzioni software Insight Control e Insight Essentials, fare clic su **Management Software and System Tools**.
- Download di driver e software (http://www.hp.com/support) – In queste pagine sono disponibili i driver e i prodotti software più recenti per i prodotti ProLiant.
- Sicurezza dei prodotti di gestione (http://www.hp.com/servers/manage/security) - HP adotta un approccio dinamico alla qualità e alla sicurezza dei propri prodotti di gestione. Controllare con regolarità la disponibilità di aggiornamenti di sicurezza scaricabili da questa sezione del sito Web HP.
- Disponibilità di nuovi CD SmartStart (http://www.hp.com/servers/smartstart) – È possibile scaricare il contenuto dei CD SmartStart, Management e Firmware effettuando una semplice procedura di registrazione sul sito Web di SmartStart. Per ricevere i CD fisici, è possibile ordinare i relativi kit dal sito Web di SmartStart. Per ricevere un messaggio di notifica ogni volta che viene rilasciato un nuovo kit SmartStart, è sufficiente effettuare l'iscrizione al servizio Subscriber's Choice (http://www.hp.com/go/subscriberschoice).

Informazioni per contattare HP

Per informazioni sul rivenditore autorizzato HP più vicino:

- Accedere al sito Web "Contact HP" (http://welcome.hp.com/country/us/en/wwcontact.html), in lingua inglese.

Per contattare l'assistenza tecnica HP:

- Negli Stati Uniti, per informazioni sulle modalità di contatto disponibili, fare riferimento alla pagina Web relativa alle informazioni di contatto per gli Stati Uniti (http://welcome.hp.com/country/us/en/contact_us.html). Per contattare HP telefonicamente:
  - Chiamare il numero 1-800-HP-INVENT (1-800-474-6836). Il servizio è disponibile 24 ore su 24, 7 giorni su 7. In accordo con la politica di miglioramento della qualità, è possibile che le telefonate siano controllate o registrate.
  - Se è stato acquistato un Care Pack (aggiornamento del servizio), chiamare il numero 1-800-633-3600. Per ulteriori informazioni sui Care Pack, visitare il sito Web HP (http://www.hp.com/hps).
- Negli altri paesi, accedere al sito Web "Contact HP" (http://welcome.hp.com/country/us/en/wwcontact.html), in lingua inglese.

Prima di contattare HP

Prima di contattare HP, assicurarsi di disporre delle seguenti informazioni:

- Numero di registrazione all'assistenza tecnica (se disponibile).
- Numero di serie del prodotto.
- Nome e numero del modello di prodotto.
- Numero di identificazione del prodotto.
- Eventuali messaggi di errore visualizzati.
- Schede o componenti hardware aggiuntivi.
- Prodotti hardware o software di terze parti.
- Tipo di sistema operativo e livello di revisione.

Acronimi e abbreviazioni

ACPI Advanced Configuration and Power Interface (Interfaccia di alimentazione e configurazione avanzata)

ARP Address Resolution Protocol (Protocollo di risoluzione degli indirizzi)

ASCII American Standard Code for Information Interchange

ASM Advanced Server Management (Gestione avanzata dei server)

ASR Automatic Server Recovery (Ripristino automatico del server)

BMC Baseboard management controller (controller di gestione baseboard)

CA Certificate Authority (Autorità di certificazione)

CLI Command Line Interface (Interfaccia della riga di comando)

CLP Command Line Protocol (Protocollo della riga di comando)

CR Certificate Request (Richiesta di certificato)

CRL Certificate Revocation List (Elenco di revoca dei certificati)

DAV Distributed Authoring and Versioning (Creazione e gestione distribuita delle versioni)

DDNS Dynamic Domain Name System (Sistema di denominazione dei domini dinamico)

DHCP Dynamic Host Configuration Protocol (Protocollo di configurazione host dinamico)

DLL Dynamic Link Library (Libreria di collegamento dinamico)

DMTF Distributed Management Task Force

DNS Domain Name System (Sistema di nomi di dominio)

DVO Digital Video Out

EAAS Environment Abnormality Auto-Shutdown (Spegnimento automatico per anomalia ambiente)

EBIPA Enclosure Bay IP Addressing (Indirizzamento IP degli alloggiamenti del contenitore)

EMS Emergency Management Services (Servizi di gestione delle emergenze)

EULA End User License Agreement (Contratto di licenza dell'utente finale)

FEH Fatal Exception Handler (Gestore di eccezioni irreversibili)

GNOME GNU Network Object Model Environment

GUI Graphical User Interface (Interfaccia utente grafica)

HB Heartbeat (Impulso vitale)

HEM High Efficiency Mode (Modalità alta efficienza)

HID Human Interface Device (Dispositivo a interfaccia umana)

HP SIM HP Systems Insight Manager

HPONCFG Utility HP Lights-Out Online Configuration (Configurazione in linea HP Lights-Out)

HPQLOMGC HP Lights-Out Migration Command Line (Riga di comando della migrazione HP Lights-Out)

HPQLOMIG HP Lights-Out Migration (Migrazione HP Lights-Out)

ICMP Internet Control Message Protocol (Protocollo dei messaggi di controllo in Internet)

iLO Integrated Lights-Out

iLO 2 Integrated Lights-Out 2

IML Integrated Management Log (Registro di gestione integrato)

IP Internet Protocol (Protocollo Internet)

IPMI Intelligent Platform Management Interface (Interfaccia di gestione della piattaforma intelligente)

IRC Integrated Remote Console (Console remota integrata)

IRQ Interrupt ReQuest (Richiesta di interrupt)

JVM Java Virtual Machine

KCS Keyboard Controller Style (Stile controller tastiera)

KDE K Desktop Environment (per Linux)

KVM Keyboard, Video, Mouse (Tastiera, video, mouse)

LAN Local-Area Network (Rete locale)

LDAP Lightweight Directory Access Protocol

LED Light-Emitting Diode (Diodo a emissione di luce)

LOM Lights-Out Management (Gestione di Lights-Out)

LSB Least Significant Bit (Bit meno significativo)

MAC Media Access Control (Controllo dell'accesso al mezzo fisico)

MLA Master License Agreement (Contratto di licenza master)

MMC Microsoft® Management Console

MP Multilink Point-to-Point Protocol

MTU Maximum Transmission Unit (Unità di trasmissione massima)

NIC Network Interface Controller (Controller d'interfaccia di rete)

NMI Non-Maskable Interrupt (Interrupt non mascherabile)

NVRAM Non-Volatile Random Access Memory (Memoria non volatile ad accesso casuale)

PERL Practical Extraction and Report Language

PKCS Public-Key Cryptography Standards (Standard di crittografia a chiave pubblica)

POST Power-On Self Test (Test automatico all'accensione)

PSP ProLiant Support Pack (Pacchetto di supporto ProLiant)

RAS Remote Access Service (Servizio di accesso remoto)

RBSU ROM-Based Setup Utility (Utility di configurazione basata sulla ROM)

RDP Remote Desktop Protocol (Protocollo desktop remoto)

RIB Remote Insight Board

RIBCL Remote Insight Board Command Language (Linguaggio di comandi Remote Insight Board)

RILOE Remote Insight Lights-Out Edition

RILOE II Remote Insight Lights-Out Edition II

ROM Read-Only Memory (Memoria di sola lettura)

RSA Rivest, Shamir, and Adelman public encryption key (Chiave di crittografia pubblica Rivest, Shamir e Adelman)

RSM Remote Server Management (Gestione remota dei server)

SAID Service Agreement Identifier (Identificativo di contratto di assistenza)

SBIPC Static Bay IP Configuration (Configurazione degli alloggiamenti con IP statico)

SLES SUSE LINUX Enterprise Server

SMASH System Management Architecture for Server Hardware (Architettura di gestione dei sistemi per l'hardware dei server)

SNMP Simple Network Management Protocol (Protocollo di gestione di rete semplice)

SSH Secure Shell

SSL Secure Sockets Layer

SSO Single Sign-On (Accesso unificato)

SUM Software Update Manager (Gestore degli aggiornamenti software)

SUV Serial, USB, Video (Seriale, USB, video)

TCP Transmission Control Protocol

TPM Trusted Platform Module (Modulo di piattaforma affidabile)

UART Universal Asynchronous Receiver-Transmitter (Ricetrasmittente asincrona universale)

UID Unit Identification (Identificazione unità)

USB Universal Serial Bus (Bus universale seriale)

VM Virtual Machine (Sistema virtuale)

VPN Virtual Private Networking (Rete privata virtuale)

VRM Voltage Regulator Module (Modulo di regolazione del voltaggio)

WINS Windows® Internet Naming Service (Servizio di denominazione Internet di Windows®)

WS Web Services (Servizi Web)

XML Extensible Markup Language

Indice analitico

B

C

D

P

R

T

U

V

W

X